THE UNIVERSITY OF WARWICK

Library Declaration and Deposit Agreement

1. STUDENT DETAILS

Please complete the following:

Full name: ……

University ID number: ……

2. THESIS DEPOSIT

2.1 I understand that under my registration at the University, I am required to deposit my thesis with the University in BOTH hard copy and in digital format. The digital version should normally be saved as a single pdf file.

2.2 The hard copy will be housed in the University Library. The digital version will be deposited in the University's Institutional Repository (WRAP). Unless otherwise indicated (see 2.3 below) this will be made openly accessible on the Internet and will be supplied to the British Library to be made available online via its Electronic Theses Online Service (EThOS) service.
[At present, theses submitted for a Master's degree by Research (MA, MSc, LLM, MS or MMedSci) are not being deposited in WRAP and not being made available via EthOS. This may change in future.]

2.3 In exceptional circumstances, the Chair of the Board of Graduate Studies may grant permission for an embargo to be placed on public access to the hard copy thesis for a limited period. It is also possible to apply separately for an embargo on the digital version. (Further information is available in the *Guide to Examinations for Higher Degrees by Research*.)

2.4 *If you are depositing a thesis for a Master's degree by Research, please complete section (a) below. For all other research degrees, please complete both sections (a) and (b) below:*

(a) Hard Copy

I hereby deposit a hard copy of my thesis in the University Library to be made publicly available to readers (please delete as appropriate) EITHER immediately OR after an embargo period of ……..... months/years as agreed by the Chair of the Board of Graduate Studies.

I agree that my thesis may be photocopied. YES / NO (*Please delete as appropriate*)

(b) Digital Copy

I hereby deposit a digital copy of my thesis to be held in WRAP and made available via EThOS.

Please choose one of the following options:

EITHER My thesis can be made publicly available online. YES / NO (*Please delete as appropriate*)

OR My thesis can be made publicly available only after…..[date] (Please give date)
YES / NO (*Please delete as appropriate*)

OR My full thesis cannot be made publicly available online but I am submitting a separately identified additional, abridged version that can be made available online.
YES / NO (*Please delete as appropriate*)

OR My thesis cannot be made publicly available online. YES / NO (*Please delete as appropriate*)

3. GRANTING OF NON-EXCLUSIVE RIGHTS

Whether I deposit my Work personally or through an assistant or other agent, I agree to the following:

Rights granted to the University of Warwick and the British Library and the user of the thesis through this agreement are non-exclusive. I retain all rights in the thesis in its present version or future versions. I agree that the institutional repository administrators and the British Library or their agents may, without changing content, digitise and migrate the thesis to any medium or format for the purpose of future preservation and accessibility.

4. DECLARATIONS

(a) I DECLARE THAT:

- I am the author and owner of the copyright in the thesis and/or I have the authority of the authors and owners of the copyright in the thesis to make this agreement. Reproduction of any part of this thesis for teaching or in academic or other forms of publication is subject to the normal limitations on the use of copyrighted materials and to the proper and full acknowledgement of its source.

- The digital version of the thesis I am supplying is the same version as the final, hard-bound copy submitted in completion of my degree, once any minor corrections have been completed.

- I have exercised reasonable care to ensure that the thesis is original, and does not to the best of my knowledge break any UK law or other Intellectual Property Right, or contain any confidential material.

- I understand that, through the medium of the Internet, files will be available to automated agents, and may be searched and copied by, for example, text mining and plagiarism detection software.

(b) IF I HAVE AGREED (in Section 2 above) TO MAKE MY THESIS PUBLICLY AVAILABLE DIGITALLY, I ALSO DECLARE THAT:

- I grant the University of Warwick and the British Library a licence to make available on the Internet the thesis in digitised format through the Institutional Repository and through the British Library via the EThOS service.

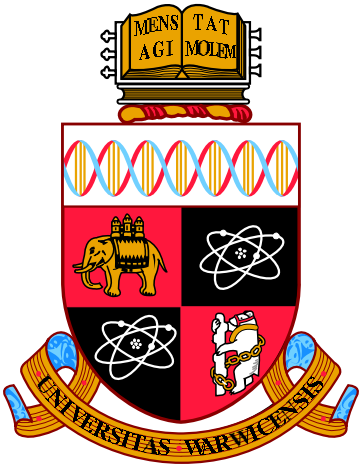
- If my thesis does include any substantial subsidiary material owned by third-party copyright holders, I have sought and obtained permission to include it in any version of my thesis available in digital format and that this permission encompasses the rights that I have granted to the University of Warwick and to the British Library.

5. LEGAL INFRINGEMENTS

I understand that neither the University of Warwick nor the British Library have any obligation to take legal action on behalf of myself, or other rights holders, in the event of infringement of intellectual property rights, breach of contract or of any other right, in the thesis.

Please sign this agreement and return it to the Graduate School Office when you submit your thesis.

Student's signature: .....…… Date: .....



Extending techniques used to determine the set of rational points on an algebraic curve

by

Michael Mourao

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Department of Mathematics

March 2013

THE UNIVERSITY OF WARWICK

Contents

Acknowledgments

My utmost gratitude goes to my supervisor, Samir Siksek, for his valuable comments and guidance. It is not possible to acknowledge in a few words the support he gave me during the past three and a half years. Without him, my research journey would not have been as exciting and rewarding as it was.

I would also like thank Brendan Creutz along with the rest of the Computational Algebra Group at the University of Sydney, for their excellent hospitality and for giving me the opportunity to include some of the algorithms described in this thesis in MAGMA [4]. My stay in Australia was one of the most memorable experiences of my life.

I am also grateful to Dino Lorenzini for pointing out that descent would be applicable to the equations in Example 2.4.2 in Chapter 2. Our correspondence gave me the much needed confidence any research student hopes to get from a much more experienced, outside observer.

My warm thanks go to my friends Stephanos Papanikolopoulos and Martha Giannoudovardi whose support included, but was not restricted to, accommodation, transportation, peer reviews, fantastic food and great company.

Many lovely memories were also due to my close friends and peers, Lassina Dembele and Nikos Zygouras. I promise that I will always keep in touch with them, no matter how far away I might be.

There would be no better place to study Number Theory than the Mathematics Department at the University of Warwick. A vibrant atmosphere was set up by John Cremona, Samir Siksek and Damiano Testa, so that a number of students and postdoctoral fellows would come together to share their passion for mathematics. I will

always cherish the moments I spent with them.

Finally, I would like to thank my mother for her constant care and attention, my father for our immensely helpful conversations, and my friends back in Cyprus: Evdokios, Iosif, Nicolas, Thomas, Thoupos and Yiannos, for providing such amazing and relaxing vacation breaks.

My research was supported by Fundação para a Ciência e Tecnologia PhD fellowship SFRH/BD/44011/2008 (QREN-POPH-Type 4.1-Advanced Training, subsidized by the European Social Fund and national funds from the Portuguese Ministry of Education and Science)

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

Declarations

Considerable effort was made to keep all the original research carried out by the author in Chapters 2 and 3 of this thesis, while including all the existing results with the appropriate references in the introductory Chapter 1. Nevertheless, there are some cases where this was not possible. For example, Lemma 1.3.32 in Chapter 1 is new, while Lemma 3.2.5 in Chapter 3 was taken from the literature. Still, the source of every statement or result is clearly stated, when this was not the author's original work.

Most of the material in Chapter 2 is identical to the material in the manuscript [39] (arXiv), written by the author of this thesis, during the period of the Ph.D. research at the University of Warwick. This was submitted for publication to a peer reviewed mathematics journal and the decision is pending.

Similarly, most of the material in Chapter 3 is identical to the material in the manuscript [38] (arXiv), written by the author of this thesis, during the period of the Ph.D. research at the University of Warwick. This was submitted for publication to a peer reviewed mathematics journal and the decision is pending.

Abstract

This thesis is concerned with the problem of determining sets of rational points on algebraic curves defined over number fields. Specifically, we will explore the methods of descent, Chabauty-Coleman and the Mordell-Weil sieve. These have been around for many years, and number theorists have used them to explicitly determine the solution sets of many interesting Diophantine equations. Here we will start by giving an introduction to the basics of the existing techniques and then proceed in the second and third chapters by providing some new insights.

In Chapter 2 we extend the method of two-cover descent on hyperelliptic curves [10], to the family of superelliptic curves. To do this, we need to get around some technical difficulties that arise from allowing these curves to have singular points. We show how to implement this process, and by doing this, we were able to apply descent to successfully compute the solutions to some interesting Diophantine problems, which we include in the end of the chapter.

Then, in Chapter 3, we extend the method of "Elliptic Curve Chabauty", introduced by Bruin in [5] and independently by Flynn and Wetherell in [21], to make it applicable on higher genus curves. To fully take advantage of this technique, we combine it with a modified version of the Mordell-Weil sieve. To demonstrate the usefulness of our approach, we determine set of $\mathbb{Q}$-rational points on a hyperelliptic curve of genus 6, after checking that the existing techniques could not be used to solve the same problem.

to my beloved brothers Nuno, Paulo and Tiago

Chapter 1

Introduction

1.1 Background

Millennia after Diophantus first started pondering about his equations, mathematicians are still trying to fully understand the secrets behind these problems whose statements are easily grasped by a non-expert, whose proofs, nevertheless, are notoriously hard to achieve.

Since Diophantine equations are essentially systems of polynomial equations, there is an obvious connection with algebraic geometry. Unlike pure geometers though, number theorists are usually interested in solution sets for these equations over fields of arithmetic nature. The interplay of the more visual realm of geometry with the discrete character of arithmetic, along with the fact that slight modifications to the constituents of a Diophantine equation usually change completely the form and complexity of the techniques needed to solve it, gave rise to some of the most beautiful mathematical developments of the past century. Probably the most notable example of this is Wiles' proof of the long standing Fermat's Last Theorem, which was based on one of the deepest connections between two seemingly unrelated areas of mathematics: elliptic curves and modular forms.

One natural invariant that helps us categorize systems of polynomial equations

is the dimension. For example, if we restrict ourselves to one dimensional varieties, or curves, we can easily reach a finer geometrical classification after considering another invariant, the genus. Every (irreducible) curve is birational to a unique non-singular curve of a given genus g, which in turn lives in a $\max\{3g-3, g\}$-dimensional moduli space of curves having the same genus. Even though curves have been studied substantially more than higher dimensional varieties, we can only claim to have a complete understanding of the behavior of the rational point sets of genus 0 curves and, if we accept the validity of the famous Birch and Swinnerton-Dyer conjecture (BSD), some might argue that we have a decent understanding of what is going on in genus 1. For higher genus curves, Faltings proved that the set of rational points is finite, but unfortunately his proof is totally ineffective.

The discovery and advancement of the computer, has also played an important role in furthering the development of arithmetic geometry. Remarkably, one of the applications of the first computer built in the United Kingdom was to test the validity of BSD. In the modern age, very few explicit computations in number theory research can be carried out by hand. Most of them require the use of highly complex algorithms and are demanding enough to put strain on supercomputers.

This thesis aims to build on several existing techniques, used to study the set of rational points on curves, in order to widen their range of applicability. Our philosophy is to be as explicit as possible, and often provide algorithms, that fully explain how the theoretical results can be implemented and used in practice.

1.2 Main results

The rest of Chapter 1 aims to remind the reader about the following topics: algebraic curves, Jacobian varieties, ramification points, points at infinity, superelliptic curves, local solubility, Hensel's lemma, the Hasse principle, descent, Coleman integration, the Chabauty-Coleman method and the Mordell-Weil sieve. All the examples included in

this chapter are either taken from the literature (e.g. Selmer's curve in Theorem 1.3.19) or straightforward applications of the existing techniques. The main results of this thesis are in Chapters 2 and 3.

In Chapter 2 we demonstrate how to perform descent on superelliptic curves. The most notable cases of Diophantine equations that were solved using this method are the four, everywhere locally soluble, equations

$$16a^7 + 87b^7 + 625c^7 = 0 \tag{1.2.1}$$

$$11a^5 + 29b^5 + 81c^5 = 0 \tag{1.2.2}$$

$$27a^5 + 16b^5 + 2209c^5 = 0 \tag{1.2.3}$$

$$32a^7 + 81b^7 + 187c^7 = 0, \tag{1.2.4}$$

whose sets of non-zero rational solutions are shown to be empty in Example 2.4.2. These were also considered in [27], but the authors stated that their methods were not applicable to these equations. Another interesting result is Theorem 2.4.5, where we show that the only pair $(a, b) \in \mathbb{Z}^2_{>0}$ satisfying the equation

$$b^3 = \sum_{i=1}^{a} i^9$$

is $(1, 1)$[1].

In Chapter 3, Theorems 3.2.3, 3.2.7 and 3.2.9 give a higher-dimensional[2] analogue of the method of "Elliptic Curve Chabauty". Combining these theorems with an appropriately extended version of the Mordell-Weil sieve (Theorem 3.3.1), we were able prove in Theorem 3.4.1, that the equation

$$y^2 = (x^3 + x^2 - 1)\Phi_{11}(x),$$

[1] This equation, along with infinite families of the same form, had already been solved (see [3], [26], [40] and [45]). Here we give an alternative proof, based on descent, that determines the full set of rational points on the corresponding curve, as opposed to the set of integral points.

[2] Or higher-genus, depending on whether one is referring to the curve or its Jacobian variety.

where Φ_{11} is the cyclotomic polynomial of degree 10, has no rational solutions[3].

1.3 Preliminaries

1.3.1 Curves and their Jacobian varieties

Throughout the thesis, C will be a projective, absolutely irreducible curve living inside some weighted M-dimensional projective space $\mathbb{P}^M(\vec{w})$, with weight vector $\vec{w} \in \mathbb{Z}_{>0}^M$. The field of definition of C will vary depending on the chapter. In this chapter C will be defined over a number field $\mathbb{K}$, possibly $\mathbb{Q}$, in Chapter 2, C will be defined over $\mathbb{Q}$ but we will use the same symbol for the extension of scalars to the fields $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$ and $\overline{\mathbb{Q}}_p$ for a rational prime p. Intrinsically, Chapter 3, relies on restriction of scalars, so C will be defined over a number field $\mathbb{K}$ strictly larger than $\mathbb{Q}$.

We fix a separable algebraic closure of $\mathbb{K}$ and denote it by $\overline{\mathbb{K}}$. Let $\mathcal{G}_{\mathbb{K}}$ be the absolute Galois group of $\mathbb{K}$. The ring of integers of $\mathbb{K}$ will be denoted by $\mathcal{O}_{\mathbb{K}}$. For an embedding $\varpi : \mathbb{A}^M \to \mathbb{P}^M(\vec{w})$, such that $\varpi(\mathbb{A}^M) \cap C \neq \emptyset$, we call $\varpi(\mathbb{A}^M) \cap C$ an affine patch of C. We denote its coordinate ring by $\overline{\mathbb{K}}[\varpi(\mathbb{A}^M) \cap C]$ (or just by $\overline{\mathbb{K}}[C]$ if the choice of affine patch is clear from the context) and its function field by $\overline{\mathbb{K}}(C) = \overline{\mathbb{K}}[\varpi(\mathbb{A}^M) \cap C]_{(0)}$, since this does not depend on the choice of ϖ. Let $\mathrm{bl} : \tilde{C} \to C$ denote the[4] desingularization of C, in other words, a non-singular projective algebraic curve over $\mathbb{K}$, birational to C i.e. with $\overline{\mathbb{K}}(\tilde{C}) \cong \overline{\mathbb{K}}(C)$. We can obtain this by performing consecutive blow-ups to get rid of the singularities, as in [23, Chapter 7]. See [23, Theorem 3 p.92] for a proof of why we only need a finite number of blow-ups to do this. For a point $P \in C$ and an affine patch $\varpi(\mathbb{A}^M) \cap C$, containing P, denote by $\mathfrak{m}_P \subset \overline{\mathbb{K}}[\varpi(\mathbb{A}^M) \cap C]$, the prime ideal consisting of functions vanishing at P and by $\overline{\mathbb{K}}[C]_P \subset \overline{\mathbb{K}}(C)$ the localization of $\overline{\mathbb{K}}[C]$ at $\mathfrak{m}_P$.

Proposition 1.3.1. *Let C be a curve over $\mathbb{K}$ and $P \in C$ a non-singular point. Then*

[3] There is of course the point at infinity on the corresponding projective curve.

[4] Uniqueness of desingularization is using the fact that C is a curve

the local ring $\overline{\mathbb{K}}[C]_P$ is a discrete valuation ring.

Proof. See for example [50, Proposition II.1.1 p. 17]. □

Definition 1.3.2. (Also in [50, p. 17]) Let C be a curve and $P \in C$ a non-singular point. The (normalized) **valuation** on $\overline{\mathbb{K}}[C]_P$ is given by

$$\mathrm{ord}_P : \overline{\mathbb{K}}[C]_P \to \{0, 1, 2, \ldots\} \cup \{\infty\}$$

$$\mathrm{ord}_P(\psi) = \max\{d \in \mathbb{Z} : \psi \in \mathfrak{m}_P^d\}.$$

Using $\mathrm{ord}_P(\psi_1/\psi_2) = \mathrm{ord}_P(\psi_1) - \mathrm{ord}_P(\psi_2)$, we extend ord_P to $\overline{\mathbb{K}}(C)$,

$$\mathrm{ord}_P : \overline{\mathbb{K}}(C) \to \mathbb{Z} \cup \{\infty\}.$$

A **uniformizer for C at P** is a function $\tau \in \overline{\mathbb{K}}(C)$ with $\mathrm{ord}_P(\tau) = 1$ (i.e. a generator for $\mathfrak{m}_P$). ⊠

Proposition 1.3.3. *Let C be a curve, $V \subset \mathbb{P}^N$ a variety, $P \in C$ a non-singular point, and $\psi : C \to V$ a rational map. Then ψ is regular at P. In particular, if C is non-singular, then ψ is a morphism.*

Proof. See for example [50, Proposition II.2.1 p. 19]. □

Definition 1.3.4. (Also in [50, p. 23]) Let $\psi : C_1 \to C_2$ be a non-constant map of non-singular curves, and let $P \in C_1$. The **ramification index of ψ at P**, denoted by $e_\psi(P)$, is given by

$$e_\psi(P) = \mathrm{ord}_P(\psi^* \tau_{\psi(P)}),$$

where $\tau_{\psi(P)} \in \overline{\mathbb{K}}(C_2)$ is a uniformizer at $\psi(P)$. Note that $e_\psi(P) \geq 1$. We say that ψ **is unramified at** P if $e_\psi(P) = 1$; and ψ **is unramified** if it is unramified at every point of C_1. ⊠

Proposition 1.3.5. *Let $\psi : C_1 \to C_2$ be a non-constant map of non-singular curves. Then for every $Q \in C_2$*

$$\sum_{P \in \psi^{-1}(Q)} e_\psi(P) = \deg(\psi).$$

Proof. Use for example [28, II.6.9]. □

Theorem 1.3.6 (Riemann-Hurwitz)**.** *Let $\psi : C_1 \to C_2$ be a non-constant map of non-singular curves which are defined over a field of characteristic zero. Then*

$$2g_1 - 2 = (\deg(\psi))(2g_2 - 2) + \sum_{P \in C_1} (e_\psi(P) - 1),$$

where g_i is the genus of C_i.

Proof. See for example [50, Theorem II.5.9 p. 37]. □

We will often use the defining equation of one of the affine patches to denote the complete curve. Even though many of the results presented here apply to a general curve, due to some, mainly computational, obstructions[5], the examples of curves given will belong to the family of superelliptic curves.

Definition 1.3.7. Let q be a rational prime and $n \geq 2$ be a positive integer. We define a **superelliptic curve** to be a projective plane curve C with an affine patch defined as the locus

$$\left\{(x, y) \in \overline{\mathbb{K}}^2 : y^q = f(x) = a_n x^n + \ldots + a_1 x + a_0\right\},$$

for some q-th power-free polynomial f with coefficients in $\mathbb{K}$. Let $\mathfrak{l}$ denote the lowest common multiple of q and n. The projective model of this superelliptic curve will be defined in the weighted projective plane $\mathbb{P}^2(\mathfrak{l}/n, \mathfrak{l}/q, 1)$ as

$$C = \left\{(X, Y, Z) \in \mathbb{P}^2(\mathfrak{l}/n, \mathfrak{l}/q, 1) : Y^q = F(X, Z) = a_n X^n + \ldots + a_1 X Z^{(\mathfrak{l}-\mathfrak{l}/n)} + a_0 Z^{\mathfrak{l}}\right\}$$

[5] For example we often need to know a finite index subgroup of the set of $\mathbb{K}$-rational points of the Jacobian variety, J, of the curve, which normally requires performing descent on J. Having said that, this has recently been achieved for other types of curves ([8]).

where the variables X, Y, Z have weights $\mathfrak{l}/n, \mathfrak{l}/q, 1$ respectively. $\boxtimes$

The choice of the ambient space for the complete model of the curve is not arbitrary and has two advantages over the completion inside the un-weighted projective plane. First, a $\mathbb{K}$-rational point (x, y) on the affine patch will satisfy $x = a/c^{\mathfrak{l}/n}, y = b/c^{\mathfrak{l}/q}$ for some $a, b, c \in \mathcal{O}_{\mathbb{K}}$. So the weighted homogeneous equation $Y^q = F(X, Z)$ can be thought of as what we get when we cancel denominators from the affine equation. Another advantage of this homogenization is that there are no singular points at infinity (i.e. points with $Z = 0$), so no need to blow-up, which would potentially change the form of the equation. We will only use this fact when $q \mid n$, in which case it is obvious when we think in terms of the affine patch $\varpi : \mathbb{A}^2 \to \mathbb{P}^2(1, n/q, 1)$, $\varpi(y, z) = (1, y, z)$.

When $q \mid n$ the superelliptic curve C has q points at infinity. Out of these

- none is $\mathbb{K}$-rational when $a_n \notin \mathbb{K}^{*q}$,
- one is $\mathbb{K}$-rational when $a_n \in \mathbb{K}^{*q}$ and 1 is the only q-th root of unity in $\mathbb{K}$,
- q are $\mathbb{K}$-rational when $a_n \in \mathbb{K}^{*q}$ and all of the q-th roots of unity are in $\mathbb{K}$.

When $q \nmid n$ there is exactly one $\mathbb{K}$-rational point at infinity. We illustrate this fact in the following example:

Example 1.3.8. ($\mathbb{K} = \mathbb{Q}$) Consider the curve

$$C : Y^3 = 8X^6 + X^3Z^3 + Z^6.$$

The points at infinity are $(1, 2, 0)$, $(1, 2\rho, 0)$ and $(1, 2\rho^2, 0)$ where ρ is a primitive cube root of unity. It is easy to see that only $(1, 2, 0)$ is $\mathbb{Q}$-rational.

Consider the curve

$$C : Y^3 = 2X^5 + X^2Z^9 + 5Z^{15}$$

Setting $Z = 0$ we see that we have the points $(1, \sqrt[3]{2}, 0)$,$(1, \rho\sqrt[3]{2}, 0)$ and $(1, \rho^2\sqrt[3]{2}, 0)$ at infinity. But actually all these are the same since

$$(1, \sqrt[3]{2}, 0) = ((\rho)^3, (\rho)^5\sqrt[3]{2}, (\rho)0) = (1, \rho^2\sqrt[3]{2}, 0) \text{ and}$$

$$(1, \sqrt[3]{2}, 0) = ((\rho^2)^3, (\rho^2)^5\sqrt[3]{2}, (\rho^2)0) = (1, \rho\sqrt[3]{2}, 0).$$

This also shows that the point at infinity is $\mathbb{Q}$-rational since it remains fixed under the action of $\mathcal{G}_{\mathbb{Q}}$. ⊠

The theory we are going to present in Chapter 2, requires a different treatment of the case $q \nmid n$, in other words when the map $\psi : C \to \mathbb{P}^1,\ (X, Y, Z) \mapsto (X, Z^{l/n})$ ramifies at the point at infinity, and the case $q \mid n$. When $q \mid n$ we can find a model of C over $\mathbb{K}$ having a ψ-ramification point at infinity only when f has a linear factor defined over $\mathbb{K}$. On the other hand, the following proposition shows that the opposite transformation is always possible, making the case $q \mid n$ more canonical, at least over non-algebraically closed fields.

Proposition 1.3.9. *Every superelliptic curve is birational to a superelliptic curve satisfying an equation of the form* $y^q = f(x)$*, where* $\deg(f) = n$ *and* $q \mid n$.

Proof. Suppose $C_{\text{old}} : y_{\text{old}}^q = f_{\text{old}}(x_{\text{old}})$ is a superelliptic curve and that $\deg(f_{\text{old}}) = m = iq + j$ with $i \in \mathbb{Z}_{\geq 0}$ and $0 \leq j < q$. Pick $a \in \mathbb{K}$ such that $f_{\text{old}}(a) \neq 0$. Define the polynomial h by $f_{\text{old}}(x_{\text{old}}) = h(x_{\text{old}} - a)$ and the polynomial f of degree $n = q(i+1)$ by $f(x) = h(1/x)x^{q(i+1)}$. Let C be the superelliptic curve defined by $y^q = f(x)$. Then C_{old} is birational to C via the map $(x_{\text{old}}, y_{\text{old}}) \mapsto \left(\frac{1}{x_{\text{old}}-a}, \frac{y_{\text{old}}}{(x_{\text{old}}-a)^{i+1}}\right)$. □

In light of this proposition, from now on we will assume that $q \mid n$.

The reason we can assume that f is q-th power-free without any loss of generality is because we have a rational map $\chi : \hat{C} \to C$ defined over $\mathbb{K}$, whenever $\hat{C}$ is given by the relation $y^q = \hat{f}(x)$ with $h^q \mid \hat{f}$ and C is given by $y^q = f(x) = \hat{f}(x)/h(x)^q$, namely

$(x, y) \mapsto (x, y/h(x))$. So it will be equivalent, if not easier due to potentially lower genus, to work with the C rather than $\hat{C}$.

The following fact appears to be well known (see for example [43, p. 148]), but we include its proof for convenience of the reader. By doing this we also explain why Theorem 1.3.6 seems to apply directly to a superelliptic curve C, even though it may be singular.

Proposition 1.3.10. *Let C be a superelliptic curve over $\mathbb{K}$ defined as in Definition 1.3.7, with $q \mid n$ and f a q-th power-free polynomial. Suppose that over $\overline{\mathbb{K}}$, f factors as*

$$f = (x - \vartheta_1)^{n_1} \dots (x - \vartheta_d)^{n_d},$$

where the ϑ_i are distinct and $1 \leq n_i < q$ for $1 \leq i \leq d$. Let $\mathrm{bl} : \tilde{C} \to C$ be the desingularization of C. Using the notation above, the genus g of C is equal to

$$g = \mathrm{Genus}(\tilde{C}) = \frac{(d-2)(q-1)}{2}.$$

Proof. Let $\psi : C \to \mathbb{P}^1$ be the morphism given by the function $x \in \left(\overline{\mathbb{K}}[x, y]/(y^q - f(x))\right)_{(0)} = \overline{\mathbb{K}}(C)$, i.e. the map that sends a point $(X, Y, Z) \in C$ to $(X, Z) \in \mathbb{P}^1$. This has degree equal to q. By Proposition 1.3.3 $\mathrm{bl} \circ \psi$ is a morphism, again of degree q, of non-singular algebraic curves. All the ramification points of $\mathrm{bl} \circ \psi$ lie in $\mathrm{bl}^{-1}(\{(X, Y, Z) \in C : Y = 0\})$. Note that $\#\{(X, Y, Z) \in C : Y = 0\} = d$. If we had that $\#\,\mathrm{bl}^{-1}(P) = 1$ for every singular point $P \in C$, i.e. all the singular points are cusps, then by Proposition 1.3.5 and Theorem 1.3.6 applied to $\mathrm{bl} \circ \psi$ we would get

$$\begin{aligned} g =& \frac{1}{2} \sum_{Q \in \tilde{C}} (e_{\mathrm{bl} \circ \psi}(Q) - 1) - q + 1 \\ =& \frac{1}{2} d(q-1) - (q-1) \\ =& \frac{(d-2)(q-1)}{2}. \end{aligned}$$

To show that this is actually the case, we need the fact that $\gcd(n_i, q) = 1$ for all $1 \leq i \leq d$. Resolving a singularity at the point $(0,0)$ of the affine patch of C of the form $y^a = x^b + O(x^{b+1})$ using consecutive blow-ups leads to an affine patch defined by the equation $y^{\gcd(a,b)} = x^{\gcd(a,b)} + h.o.t.$ This is analogous to the way one performs the Euclidean algorithm on a and b. This means, after we resolve the remaining singularity, we will have exactly $\gcd(a,b)$ points on $\tilde{C}$ that map to $(0,0)$ on C. In our case $a = q$ and $b = n_i$, so we have exactly one. A similar argument can be used for singularities away from the origin. □

We have the following inclusions:

$$\left\{ \begin{array}{c} \text{Elliptic curves} \\ q = 2, n = 3 \\ \text{or} \\ q = 2, n = 4, C(\mathbb{K}) \neq \emptyset \end{array} \right\} \subset \left\{ \begin{array}{c} \text{Superelliptic} \\ \text{curves} \end{array} \right\} \supset \left\{ \begin{array}{c} \text{Hyperelliptic} \\ \text{curves} \\ q = 2, n > 4 \end{array} \right\}.$$

It is well known that for elliptic curves, the set of points $C(\overline{\mathbb{K}})$ can be given the structure of an abelian group and for any intermediate field $\mathbb{K} \subseteq \mathbb{K}^{\text{ext}} \subseteq \overline{\mathbb{K}}$, the set of $\mathbb{K}^{\text{ext}}$-rational points $C(\mathbb{K}^{\text{ext}})$ is a subgroup of $C(\overline{\mathbb{K}})$. For an arbitrary curve C over $\mathbb{K}$ of genus $g > 1$ one can define the free abelian group of divisors $\text{Div}_{\overline{\mathbb{K}}}(C)$ and its subgroup $\text{Princ}_{\overline{\mathbb{K}}}(C)$ of principal divisors. Let $\text{Div}^0_{\overline{\mathbb{K}}}(C)$ denote the kernel of the degree map $\deg : \text{Div}_{\overline{\mathbb{K}}}(C) \to \mathbb{Z}$. The Picard group $\text{Pic}_{\overline{\mathbb{K}}}(C)$ is the quotient $\text{Div}_{\overline{\mathbb{K}}}(C)/\,\text{Princ}_{\overline{\mathbb{K}}}(C)$. Since deg is zero on $\text{Princ}_{\overline{\mathbb{K}}}(C)$, it reduces to $\text{Pic}_{\overline{\mathbb{K}}}(C)$. The kernel of $\deg : \text{Pic}_{\overline{\mathbb{K}}}(C) \to \mathbb{Z}$ is denoted by $\text{Pic}^0_{\overline{\mathbb{K}}}(C)$. When C is non-singular $\text{Pic}^0_{\overline{\mathbb{K}}}(C)$ can be given the structure of a projective abelian variety defined over $\mathbb{K}$ ([12]). This is called the Jacobian variety of the curve C and we denote it by J. Now as far as $\mathbb{K}$-rationality is concerned we define

- $\text{Div}_{\mathbb{K}}(C) = \text{Div}_{\overline{\mathbb{K}}}(C)^{\mathcal{G}_{\mathbb{K}}}$ (${}^{\mathcal{G}_{\mathbb{K}}}$ denotes the part fixed by the $\mathcal{G}_{\mathbb{K}}$-action),
- $\text{Princ}_{\mathbb{K}}(C) = \text{Princ}_{\overline{\mathbb{K}}}(C)^{\mathcal{G}_{\mathbb{K}}}$,

- $\mathrm{Pic}_{\mathbb{K}}(C) = \mathrm{Div}_{\mathbb{K}}(C)/\mathrm{Princ}_{\mathbb{K}}(C)$,
- $\mathrm{Pic}^0_{\mathbb{K}}(C) = \mathrm{Kernel}(\deg : \mathrm{Pic}_{\mathbb{K}}(C) \to \mathbb{Z})$ and
- $J(\mathbb{K}) = \mathrm{Pic}^0_{\overline{\mathbb{K}}}(C)^{\mathcal{G}_{\mathbb{K}}}$, the subgroup of $\mathbb{K}$-rational points on the Jacobian variety.

Note that the map $\mathrm{Pic}^0_{\mathbb{K}}(C) \to J(\mathbb{K})$ is injective but not always surjective, since a $\mathbb{K}$-rational divisor class might not contain a $\mathbb{K}$-rational divisor. When $C(\mathbb{K}) \neq \emptyset$ this map is indeed an isomorphism (see for example [43, Proposition 3.2]).

Notation 1.3.11. Let V be a reduced, absolutely irreducible, projective variety defined over a number field $\mathbb{K}$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$. We denote by $V_{\mathfrak{p}}$ the base change of V to the completion $\mathbb{K}_{\mathfrak{p}}$ of $\mathbb{K}$ with respect to the non-archimedean place corresponding to $\mathfrak{p}$ and by $\overline{V}_{\mathfrak{p}}$ the variety over the finite field $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ obtained by reducing the coefficients of $V_{\mathfrak{p}}$ modulo $\mathfrak{p}$. We then have a reduction map

$$\mathrm{red}_{\mathfrak{p}} : V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \to \overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}),$$

which is also a homomorphism whenever V is an abelian variety. We will denote the restriction of this map to $V(\mathbb{K})$ by $\mathrm{Red}_{\mathfrak{p}}$.

When we have a finite number field extension $\mathbb{Q} \subset \mathbb{K}$ and p is a rational prime, we will denote by

$$\mathrm{Red}_p : V(\mathbb{K}) \to \prod_{\mathfrak{p}|p} \overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$$

the map sending a $\mathbb{K}$-rational point P to the tuple $(\mathrm{Red}_{\mathfrak{p}}(P))_{\mathfrak{p}|p}$, where $\mathfrak{p}$ runs through all the primes of $\mathcal{O}_{\mathbb{K}}$ that divide p. ⊠

Now we will state some important results we will be using later. The first, Theorem 1.3.12 is a bound on the number of rational points on a non-singular curve over a finite field. We can interpret this bound roughly as saying that a non-singular curve of genus g over a field with p^a elements has approximately as many points as the projective line over that field, namely $p^a + 1$, modulo an error which can be bounded in terms of

g. This inequality is a consequence of the "Riemann Hypothesis" part of the famous Weil Conjectures (for the case of curves). The second, Theorem 1.3.13, is a statement concerning the finite generation of the group of rational points on an abelian variety. We will be using it in the case where $\mathcal{A} = J$, the Jacobian of a non-singular curve C. Last, but certainly not least, is Theorem 1.3.14, originally known as "Mordell's Conjecture", and proved by Faltings in 1983. It states that for curves C of genus $g > 1$ defined over a number field $\mathbb{K}$, we have $\#C(\mathbb{K}) < \infty$. Even though we will not be using this per se, as it is ineffective, it is nevertheless the main reason the techniques developed here are meaningful.

Theorem 1.3.12 (Hasse-Weil). *Let p be a rational prime, a a positive integer and C be a non-singular curve over the finite field $\mathbb{F}$ with p^a elements. Then*

$$| C(\mathbb{F}) - p^a - 1 | \leq 2g\sqrt{p^a},$$

where g is the genus of C.

Proof. See [55]. □

Theorem 1.3.13 (Mordell-Weil). *Let $\mathcal{A}$ be an abelian variety defined over a number field $\mathbb{K}$. Then the set of $\mathbb{K}$-rational points $\mathcal{A}(\mathbb{K})$ is a finitely generated abelian group i.e.*

$$\mathcal{A}(\mathbb{K}) \cong \mathbb{T} \oplus \mathbb{Z}^r,$$

where $\mathbb{T}$ is a finite abelian group, the torsion subgroup, and r a non-negative integer, the rank.

Proof. For elliptic curves over $\mathbb{Q}$ see [37] and for the extension to abelian varieties over number fields see [54]. □

Theorem 1.3.14 (Faltings). *Let C be a non-singular curve defined over a number field $\mathbb{K}$. When the genus of C is greater than 1, the set of $\mathbb{K}$-rational points $C(\mathbb{K})$ is finite.*

Proof. This was first proved by Faltings in [19]. □

1.3.2 Hasse's local-to-global principle

Let V be a variety over a number field $\mathbb{K}$ and let $\mathfrak{v}$ be a place of $\mathbb{K}$ (finite or infinite). Then the embedding of $\overline{\mathbb{K}}$ in its completion $\overline{\mathbb{K}}_{\mathfrak{v}}$ induces an embedding of $V(\mathbb{K})$ in $V_{\mathfrak{v}}(\mathbb{K}_{\mathfrak{v}})$. So we have the following straightforward implication

$$V_{\mathfrak{v}}(\mathbb{K}_v) = \emptyset \text{ for some place } \mathfrak{v} \Rightarrow V(\mathbb{K}) = \emptyset,$$

which can be thought of as the first tool available for proving that the set $V(\mathbb{K})$ is empty. For a while mathematicians believed that a converse of this statement, namely

$$V_{\mathfrak{v}}(\mathbb{K}_{\mathfrak{v}}) \neq \emptyset \text{ for all places } \mathfrak{v} \Rightarrow V(\mathbb{K}) \neq \emptyset, \tag{1.3.1}$$

was also true, and actually Hasse in his doctoral thesis proved the following theorem:

Theorem 1.3.15 (Hasse-Minkowski)**.** *Let n be any positive integer and $Q(x_1, \ldots, x_n)$ be a quadratic form over $\mathbb{Q}$. The equation*

$$Q(x_1, \ldots, x_n) = 0$$

has a non-trivial solution if and only if it has a non-trivial solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p.

Proof. See [29]. □

Hasse later generalized this to any number field and asked whether this is true in general. Since then, varieties V that satisfy (1.3.1) are said to satisfy the Hasse principle.

Violations to the Hasse principle were given by Lind [34], Reichardt [44] for the

case of inhomogeneous quartic equations such as

$$2Y^2 = X^4 - 17Z^4$$

and later Selmer in [47] presented extensive tables of violations in the case of homogeneous cubics in three variables, with the simplest example being

$$3X^3 + 4Y^3 + 5Z^3 = 0. \tag{1.3.2}$$

Before we present a proof that (1.3.2) has no rational solutions, let us first state and prove a simple, yet essential, result justifying the algorithmic nature of the determination of whether $V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ is empty or not for a finite place $\mathfrak{p}$ of $\mathbb{K}$. It is basically a generalization of the Newton-Raphson method for root approximation in $\mathbb{R}$ to the case of complete local fields.

Lemma 1.3.16 (Hensel [30])**.** *Let $\mathbb{K}_{\mathfrak{p}}$ be the completion of a number field $\mathbb{K}$ with respect to the discrete valuation $\mathrm{ord}_{\mathfrak{p}} : \mathbb{K}_{\mathfrak{p}} \to \mathbb{Z} \cup \{\infty\}$ corresponding to the non-archimedean place $\mathfrak{p}$, and $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ be its ring of integers. If F is a polynomial with coefficients in $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ and $w \in \mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ satisfies*

$$\mathrm{ord}_{\mathfrak{p}}(F(w)) \geq 2\,\mathrm{ord}_{\mathfrak{p}}(F'(w)) + 1$$

where F' is the formal derivative of F, then there exists a unique $\hat{w} \in \mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ with $F(\hat{w}) = 0$ and $\mathrm{ord}_p(\hat{w} - w) \geq \mathrm{ord}_{\mathfrak{p}}\left(\frac{F(w)}{F'(w)}\right)$.

Proof. (The proof of this is straightforward and very well known, but we present it here since it will be used extensively later on.) Let $w_0 = w$ and for $i \geq 1$ define recursively $w_i = w_{i-1} - \xi_{i-1}$ where $\xi_{i-1} = \frac{F(w_{i-1})}{F'(w_{i-1})}$. We will show that $\{w_i\}_{i=0}^{\infty}$ is a sequence in $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ that converges to an $\hat{w} \in \mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ satisfying the conditions in the statement of the lemma. First we show that for each i, $\mathrm{ord}_{\mathfrak{p}}(F(w_i)) > \mathrm{ord}_{\mathfrak{p}}(F(w_{i-1}))$, $\mathrm{ord}_{\mathfrak{p}}(F'(w_i)) = \mathrm{ord}_{\mathfrak{p}}(F'(w_{i-1}))$ and $\mathrm{ord}_{\mathfrak{p}}(F(w_i)) \geq 2\,\mathrm{ord}_{\mathfrak{p}}(F'(w_i)) + 1$. We will do this using induction.

For $i = 1$ consider the Taylor expansion

$$F(w_1) = F(w_0 - \xi_0) = F(w_0) - F'(w_0)\frac{F(w_0)}{F'(w_0)} + O(\xi_0^2) = O(\xi_0^2).$$

Note that $\mathrm{ord}_{\mathfrak{p}}(F(w_1)) \geq 2(\mathrm{ord}_{\mathfrak{p}}(F(w_0)) - \mathrm{ord}_{\mathfrak{p}}(F'(w_0))) > \mathrm{ord}_{\mathfrak{p}}(F(w_0))$ and

$$F'(w_1) = F'(w_0) + O(\xi_0)$$

so $\mathrm{ord}_{\mathfrak{p}}(F'(w_1)) = \mathrm{ord}_{\mathfrak{p}}(F'(w_0))$. Combining these, we see that

$$\mathrm{ord}_{\mathfrak{p}}(F(w_1)) > \mathrm{ord}_{\mathfrak{p}}(F(w_0)) \geq 2\,\mathrm{ord}_p(F'(w_0)) + 1 = 2\,\mathrm{ord}_{\mathfrak{p}}(F'(w_1)) + 1$$

as required. The inductive step can be shown using exactly the same arguments, just replacing the indices 0 by $i-1$ and 1 by i. As i increases the valuation of $F(w_i)$ increases (strictly) while the valuation of $F'(w_i)$ stays the same, so

$$\lim_{i\to\infty} \mathrm{ord}_{\mathfrak{p}}(w_i - w_{i-1}) = \lim_{i\to\infty} \mathrm{ord}_{\mathfrak{p}}(-\xi_i) = \infty.$$

In other words, $\{w_i\}_{i=0}^{\infty}$ is a Cauchy sequence, and since $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ is complete, we have that $\lim_{i\to\infty} w_i$ exists. We call this limit $\hat{w}$. By continuity of F and F' we also have

$$\mathrm{ord}_{\mathfrak{p}}(F(\hat{w})) = \mathrm{ord}_{\mathfrak{p}}(F(\lim_{i\to\infty} w_i)) = \lim_{i\to\infty} \mathrm{ord}_{\mathfrak{p}}(F(w_i)) = \infty, \tag{1.3.3}$$

$$\mathrm{ord}_{\mathfrak{p}}(F'(\hat{w})) = \mathrm{ord}_{\mathfrak{p}}(F'(\lim_{i\to\infty} w_i)) = \lim_{i\to\infty} \mathrm{ord}_{\mathfrak{p}}(F'(w_i)) = \mathrm{ord}_{\mathfrak{p}}(F'(w)) \tag{1.3.4}$$

and

$$\mathrm{ord}_{\mathfrak{p}}(\hat{w} - w) = \mathrm{ord}_{\mathfrak{p}}(\lim_{i\to\infty} w_i - w) = \lim_{i\to\infty} \mathrm{ord}_{\mathfrak{p}}\left(-\sum_{j=0}^{i} \xi_j\right) = \mathrm{ord}_{\mathfrak{p}}(\xi_0). \tag{1.3.5}$$

By (1.3.3) and (1.3.5) we get that $F(\hat{w}) = 0$ and $\mathrm{ord}_{\mathfrak{p}}(\hat{w}-w) \geq \mathrm{ord}_{\mathfrak{p}}\left(\frac{F(w)}{F'(w)}\right)$ which proves

the existence part of the lemma. For uniqueness, note that if there exists $w^* \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ with $F(w^*) = 0$ and $\mathrm{ord}_\mathfrak{p}(w^* - w) \geq \mathrm{ord}_\mathfrak{p}\left(\frac{F(w)}{F'(w)}\right)$ then there exists $u \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ such that $w^* = \hat{w} + u\frac{F(w)}{F'(w)}$ and the Taylor expansion

$$0 = F(w^*) = F(\hat{w}) + uF'(\hat{w})\frac{F(w)}{F'(w)} + O\left(\left(u\frac{F(w)}{F'(w)}\right)^2\right),$$

together with (1.3.4) show that $u = 0$. □

Lemma 1.3.17. *Equation* (1.3.2) *has solutions everywhere locally.*

Proof. The existence of solutions over $\mathbb{R}$ is obvious due to the odd degree of the equation. To deal with the non-archimedean places, note that (1.3.2) defines a curve C of genus 1 in $\mathbb{P}^2$, with 2, 3 and 5 being the primes where C has bad reduction, so Theorem 1.3.12, which ensures that $\overline{C}_p(\mathbb{F}_p) \neq \emptyset$, can be combined with Hensel's lemma to deduce that $C_p(\mathbb{Q}_p) \neq \emptyset$ for primes $p \geq 7$. To see this, suppose $(X, Y, 1) \in \overline{C}(\mathbb{F}_p)$, let $\hat{X}, \hat{Y}$ be any lifts of X, Y to $\mathbb{Z}_p$, and set either $\{F(x) = 3x^3 + 4\hat{Y}^3 + 5, w = \hat{X}\}$ or $\{F(y) = 3\hat{X}^3 + 4y^3 + 5, w = \hat{Y}\}$ in the proof of Lemma 1.3.16 (the choice is made so that $F'(w)$ does not evaluate to zero modulo p). To show local solubility for the remaining primes, we can use an extension[6] of Lemma 1.3.16 to bivariate polynomials which define affine patches of superelliptic curves with bad reduction at p. □

Lemma 1.3.18. *Equation* (1.3.2) *has no non-zero solution* $(X, Y, Z) \in \mathbb{Z}^3$. *Equivalently, when this solution set is thought of as the set of* $\mathbb{Q}$*-rational points of the curve* C *defined by the same equation in* $\mathbb{P}^2$, *then* $C(\mathbb{Q}) = \emptyset$.

Proof. We first use the automorphism of $\mathbb{P}^2$, $(X, Y, Z) \mapsto (3X, -6Y, Z)$ to bring C into the superelliptic form

$$C : Y^3 = 6(X^3 + 45Z^3).$$

[6]Since lifting arguments of this type are well known, but quite messy, we do not include it here. For details and implementation see `http://www.warwick.ac.uk/~marfaq/els.m`.

After scaling a point $P = (X, Y, Z) \in C(\mathbb{Q})$, we may assume that X, Y and Z are coprime integers. Let K be the number field $\mathbb{Q}[t]/(t^3 + 45)$ and θ be the image of the generator t in K. Suppose that $\mathfrak{p}$ is a prime of the ring of integers $\mathcal{O}_K$ such that $\mathfrak{p} \nmid 6$ and $3 \nmid \mathrm{ord}_{\mathfrak{p}}(X - \theta Z)$, in particular

$$X \equiv \theta Z \mod \mathfrak{p}. \tag{1.3.6}$$

Then since $3 \mid \mathrm{ord}_{\mathfrak{p}}(Y^3) = \mathrm{ord}_{\mathfrak{p}}(6) + \mathrm{ord}_{\mathfrak{p}}(X - \theta Z) + \mathrm{ord}_{\mathfrak{p}}(X^2 + \theta XZ + \theta^2 Z^2)$, we also have that $3 \nmid \mathrm{ord}_{\mathfrak{p}}(X^2 + \theta XZ + \theta^2 Z^2)$, in particular

$$X^2 + \theta XZ + \theta^2 Z^2 \equiv 0 \mod \mathfrak{p}. \tag{1.3.7}$$

Combining (1.3.6) and (1.3.7) we get that

$$3\theta^2 Z^2 \equiv 0 \mod \mathfrak{p}.$$

and we can deduce that $\mathfrak{p} \mid 3\theta^2$ since X and Z are coprime. By dropping the condition $\mathfrak{p} \nmid 6$ we get that

$$\begin{aligned} 3 \nmid \mathrm{ord}_{\mathfrak{p}}(X - \theta Z) &\Rightarrow \mathfrak{p} \mid 6\theta^2 \\ &\Rightarrow \mathfrak{p} \in \{\mathfrak{p}_{2,1}, \mathfrak{p}_{2,2}, \mathfrak{p}_3, \mathfrak{p}_5\} = \mathrm{Supp}(6\theta^2 \mathcal{O}_K). \end{aligned}$$

Thus for every point $(X, Y, Z) \in C(\mathbb{Q})$ we have an equality of ideals

$$(X - \theta Z)\mathcal{O}_K = \mathfrak{p}_{2,1}^{e_1} \mathfrak{p}_{2,2}^{e_2} \mathfrak{p}_3^{e_3} \mathfrak{p}_5^{e_4} \mathcal{I}^3$$

where $e_i \in \{0, 1, 2\}$ and $\mathcal{I}$ is an ideal of $\mathcal{O}_K$. Let ϵ be the fundamental unit of K and g_1, g_2, g_3, g_4 be generators of $\mathfrak{p}_{2,1}, \mathfrak{p}_{2,2}, \mathfrak{p}_3, \mathfrak{p}_5$ respectively (K has class number 1). Then

there exist $e_i \in \{0,1,2\}$ $0 \leq i \leq 4$ and $u_0, u_1, u_2 \in \mathbb{Z}$ such that

$$X - \theta Z = \epsilon^{e_0} g_1^{e_1} g_2^{e_2} g_3^{e_3} g_4^{e_4} (u_0 + u_1\theta + u_2\theta^2)^3. \tag{1.3.8}$$

Denote the tuple $(e_0, \ldots, e_4)$ by $\mathbf{e}$ and $\epsilon^{e_0} g_1^{e_1} g_2^{e_2} g_3^{e_3} g_4^{e_4}$ by $\alpha_{\mathbf{e}}$. We have

$$\frac{Y^3}{6} = \mathcal{N}_{K/\mathbb{Q}}(X - \theta Z) = \mathcal{N}_{K/\mathbb{Q}}(\alpha_{\mathbf{e}}) s^3,$$

so $6\mathcal{N}_{K/\mathbb{Q}}(\alpha_{\mathbf{e}}) \in \mathbb{Q}^{*3}$. This fact allows us to exclude all apart from 3^2 of the 3^5 possible $\mathbf{e}$'s. For a point $P = (X, Y, Z) \in C(\mathbb{Q})$ we say that $\alpha_{\mathbf{e}}$ covers P when (1.3.8) holds for some $\mathbf{u} = (u_0, u_1, u_2) \in \mathbb{P}^2$ (here we drop the assumption that X, Y and Z are coprime integers and we allow scaling of the point). Then it is not hard to see that when we have $\alpha_{\mathbf{e}_1} = \lambda \alpha_{\mathbf{e}_2} \beta^3$ for some $\lambda \in \mathbb{Q}^*, \beta \in K^*$, we have that $\alpha_{\mathbf{e}_1}$ covers P if and only if $\alpha_{\mathbf{e}_2}$ covers P (we can use λ to scale P and β to transform linearly from one triple $\mathbf{u}$ to the other). Using this allows us to deduce that the 9 remaining $\alpha_{\mathbf{e}}$'s all cover the same elements of $C(\mathbb{Q})$. Note also that by our initial construction every element of $C(\mathbb{Q})$ is covered by an $\alpha_{\mathbf{e}}$ for some $\mathbf{e}$. Thus, for $C(\mathbb{Q})$ to be empty, we only need to show that any of the 9 remaining $\alpha_{\mathbf{e}}$'s cannot cover a point on C, i.e. the corresponding $\mathbf{u}$ does not exist. For $\mathbf{e} = (0, 1, 0, 2, 0)$ we have $\alpha_{\mathbf{e}} = \theta^2 + \theta - 9$, with $\mathcal{N}_{K/\mathbb{Q}}(\alpha_{\mathbf{e}}) = 36$. After expanding (1.3.8) for this $\alpha_{\mathbf{e}}$ we get

$$X - \theta Z = W_0(\mathbf{u}) + W_1(\mathbf{u})\theta + W_2(\mathbf{u})\theta^2,$$

where W_0, W_1 and W_2 are cubic forms in three variables with coefficients in $\mathbb{Q}$. From what we have so far, for $C(\mathbb{Q})$ to be non-empty we must have a non-zero solution $\mathbf{u}$ to the equation

$$W_2(\mathbf{u}) = 0. \tag{1.3.9}$$

In other words we must have

$$u_0^3 + 3u_0^2u_1 - 27u_0^2u_2 - 27u_0u_1^2 - 270u_0u_1u_2 - 135u_0u_2^2 - 45u_1^3 - 135u_1^2u_2 + 1215u_1u_2^2 + 2025u_2^3 = 0. \quad (1.3.10)$$

By scaling we may assume u_0, u_1 and u_2 are coprime. By (1.3.10) we deduce that $3 \mid u_0$, so $u_0 = 3v_0$ and we must have

$$3v_0^3 + 3v_0^2u_1 - 27v_0^2u_2 - 9v_0u_1^2 - 90v_0u_1u_2 - 45v_0u_2^2 - 5u_1^3 - 15u_1^2u_2 + 135u_1u_2^2 + 225u_2^3 = 0. \quad (1.3.11)$$

Now (1.3.11) implies that $3 \mid u_1$, so $u_1 = 3v_1$ and substituting in (1.3.11) gives

$$v_0^3 + 3v0^2v_1 - 9v_0^2u_2 - 27v_0v_1^2 - 90v_0v_1u_2 - 15v_0u_2^2 - 45v_1^3 - 45v_1^2u_2 + 135v_1u_2^2 + 75u_2^3 = 0, \quad (1.3.12)$$

which in turn implies that $3 \mid v_0$, so $v_0 = 3w_0$ and we get

$$9w_0^3 + 9w_0^2v_1 - 27w_0^2u_2 - 27w_0v_1^2 - 90w_0v_1u_2 - 15w_0u_2^2 - 15v_1^3 - 15v_1^2u_2 + 45v_1u_2^2 + 25u_2^3 = 0. \quad (1.3.13)$$

Finally (1.3.13) implies that $3 \mid u_2$, which leads to a contradiction. This argument essentially shows that there are no solutions in $\mathbb{Q}_3$, thus (1.3.9) has no solutions in $\mathbb{Q}$. □

Lemmas 1.3.17 and 1.3.18 together constitute a proof that Selmer's example is actually a violation of Hasse's local-to-global principle.

Theorem 1.3.19. *The equation*

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

has solutions everywhere locally, but fails to have a rational solution.

We should note that this might not be exactly the same proof that Selmer gave, but it is based on the same idea, adjusted to prelude the descent arguments that will appear later.

Already apparent in the proof of Lemma 1.3.18 is the geometry behind the method of descent. We will soon give a more concrete description of the geometric constructions used in the general case and see how these provide very useful insights on how to deal with number theoretic problems.

1.3.3 Chabauty-Coleman

Back in 1941, probably while trying to prove Mordell's Conjecture (i.e. Theorem 1.3.14), Chabauty in [11] had the idea of using integration on $C_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ and $J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ for a curve C defined over $\mathbb{K}$ and its Jacobian J. While his method was only applicable to curves whose genus g was strictly greater than the Mordell-Weil rank r, thus failing to prove the whole conjecture, unlike Faltings' proof, Chabauty's argument could be made effective[7]. This was noted by Coleman in [13], after he set well established foundations for computing the necessary integrals in [14]. A very well written exposition can be found in [36]. In this section we will remind the reader about the basics behind the Chabauty-Coleman method and also present how one would perform it explicitly to determine the set of rational points in particular cases.

Let us start by setting up the necessary notation.

Notation 1.3.20. We will use $H^0(V_{\mathfrak{p}}, \Omega^1)$ to denote the $\mathbb{K}_{\mathfrak{p}}$-vector space of regular 1-

[7] Effective here means: Can be used to obtain bounds for the number of rational points on curves defined over number fields.

forms on the base change of a variety V with respect to a prime $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$. For a subset $S \subseteq V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ let S^{cl} denote the ($\mathfrak{p}$-adic) closure of S in $V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$. ⊠

We will assume the existence of a point $P_0 \in C(\mathbb{K})$. As we will see later, the technique discussed in this section is useless in showing that $C(\mathbb{K}) = \emptyset$, so the assumption comes essentially without any loss of generality. We use P_0 to define the Abel-Jacobi embedding

$$\iota : C \to J, \quad \iota(P) = [P - P_0],$$

which gives rise to an isomorphism of g-dimensional $\mathbb{K}_{\mathfrak{p}}$-vector spaces

$$\iota^* : H^0(J_{\mathfrak{p}}, \Omega^1) \to H^0(C_{\mathfrak{p}}, \Omega^1).$$

Definition 1.3.21. For a finite extension $\mathbb{K}$ of $\mathbb{Q}$ and a prime $\mathfrak{p}$ of $\mathbb{K}$ above a prime p of $\mathbb{Q}$ we define the **ultrametric absolute value on** $\mathbb{K}_{\mathfrak{p}}$ to be

$$|\cdot| : \mathbb{K}_{\mathfrak{p}} \to \mathbb{R},$$

$$|a| = p^{-\frac{\mathrm{ord}_p\left(\mathcal{N}_{\mathbb{K}_{\mathfrak{p}}/\mathbb{Q}_p}(a)\right)}{[\mathbb{K}_{\mathfrak{p}}:\mathbb{Q}_p]}}.$$

Also for any $m \in \mathbb{Z}_{\geq 1}$ we define

$$\|\cdot\| : \mathbb{K}_{\mathfrak{p}}^m \to \mathbb{R},$$

$$\|(a_1, \ldots, a_m)\| = \max_{1 \leq i \leq m} |\, a_i \,|$$

and for $\epsilon > 0$ the **open polydisc centered at the origin**

$$\mathcal{B}_{\mathfrak{p}}(\epsilon, m) = \left\{ \mathbf{a} \in \mathbb{K}_{\mathfrak{p}}^m : \|\mathbf{a}\| < \epsilon \right\}.$$

⊠

Definition 1.3.22. For $m \in \mathbb{Z}_{\geq 1}$ let $\mathrm{PS}_{\mathfrak{p}}(m)$ denote the formal powerseries ring in m variables with coefficients in $\mathbb{K}_{\mathfrak{p}}$ and for $\epsilon > 0$ let $\mathrm{PS}_{\mathfrak{p}}(\epsilon, m)$ be the **subring of ϵ-convergent powerseries**, i.e.

$$\sum_{\mathbf{i} \in \mathbb{Z}^m_{\geq 0}} c_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathrm{PS}_{\mathfrak{p}}(\epsilon, m) \quad \text{if and only if}$$

$$\lim_{\deg(\mathbf{i}) \to \infty} \epsilon^{\deg(\mathbf{i})} |c_{\mathbf{i}}| = 0,$$

where $\deg(\mathbf{i}) = \deg((i_1, \ldots, i_m)) = i_1 + \ldots + i_m$. ⊠

Lemma 1.3.23. *Let $\mathfrak{p}$ be an unramified prime of $\mathbb{K}$ above a rational prime p. Suppose that $I \in \mathrm{PS}_{\mathfrak{p}}(1,1)$ is such that all the coefficients of its formal derivative I' are in $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$. Let k be the order of vanishing at zero of the reduction $\overline{I'}$ modulo $\mathfrak{p}$. If $k < p-2$, then I has at most $k+1$ zeros in $\mathfrak{p}\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$.*

Proof. See for example [36, Lemma 5.1] for $\mathbb{K} = \mathbb{Q}$. The proof here is the same since $\mathfrak{p}$ is unramified. □

Definition 1.3.24. Let $V_{\mathfrak{p}}$ be a non-singular projective variety of dimension m over $\mathbb{K}_{\mathfrak{p}}$ with good reduction. We say that a function $\eta : V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \to \mathbb{K}_{\mathfrak{p}}$ is **locally analytic** if for every $P \in V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ there exists a subset $U \subset V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ containing P and local parameters $\tau_1, \ldots, \tau_m \in \mathbb{K}_{\mathfrak{p}}(V_{\mathfrak{p}})$ giving an isomorphism $\tau = (\tau_1, \ldots, \tau_m) : U \to \mathcal{B}_{\mathfrak{p}}(\epsilon, m)$, sending P to the origin, for some $\epsilon > 0$, together with an ϵ-convergent powerseries $I \in \mathrm{PS}_{\mathfrak{p}}(\epsilon, m)$ such that

$$\eta(P') = I(\tau(P'))$$

for all $P' \in U$. ⊠

Theorem 1.3.25. *Let $V_{\mathfrak{p}}$ be a non-singular projective variety of good reduction defined over $\mathbb{K}_{\mathfrak{p}}$ and $\omega \in H^0(V_{\mathfrak{p}}, \Omega^1)$ be a regular, closed 1-form. Then there exists a locally analytic function, $\eta_\omega : V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \to \mathbb{K}_{\mathfrak{p}}$, unique up to additive constant, such that $d\eta_\omega = \omega$.*

For $P, Q \in V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$ we set $\int_P^Q \omega = \eta_\omega(Q) - \eta_\omega(P)$. This integral satisfies the following properties:

Additivity *For $\omega_1, \omega_2 \in H^0(V_{\mathfrak{p}}, \Omega^1)$*

$$\int_P^Q (\omega_1 + \omega_2) = \int_P^Q \omega_1 + \int_P^Q \omega_2.$$

Fundamental Theorem of Calculus *If $\omega = d\psi$ for some $\psi \in \mathbb{K}_{\mathfrak{p}}(V_{\mathfrak{p}})$ then*

$$\int_P^Q \omega = \psi(Q) - \psi(P).$$

Change of Variables *Suppose $\iota : V'_{\mathfrak{p}} \to V_{\mathfrak{p}}$ is a morphism of non-singular projective varieties of good reduction over $\mathbb{K}_{\mathfrak{p}}$ then*

$$\int_P^Q \iota^*\omega = \int_{\iota(P)}^{\iota(Q)} \omega.$$

Homomorphism *If $V_{\mathfrak{p}}$ is also an abelian variety then*

$$\eta_\omega^+ := \int_0^\bullet \omega : V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \to (\mathbb{K}_{\mathfrak{p}}, +)$$

is a homomorphism of abelian groups.

Proof. See [14, Section II]. □

The following straightforward corollary will prove to be useful later:

Corollary 1.3.26. *Let $\iota : C \to J$ be the Abel-Jacobi embedding with basepoint P_0 and $P \in C(\mathbb{K})$ be a rational point such that $N \cdot \iota(P) = \sum_{i=1}^r n_i D_i$ for $N, n_1, \ldots, n_r \in \mathbb{Z}$, $N \neq 0$, $D_1, \ldots, D_r \in J(\mathbb{K})$ and $\omega \in H^0(J_{\mathfrak{p}}, \Omega^1)$ for some prime $\mathfrak{p}$ of good reduction. Then*

$$\int_{P_0}^P \iota^*\omega = \frac{1}{N}\left(\sum_{i=1}^r n_i \int_0^{D_i} \omega\right).$$

Proof. We have that

$$N\int_{P_0}^{P}\iota^*\omega = N\int_0^{\iota(P)}\omega = \int_0^{N\cdot\iota(P)}\omega$$

by the change of variables and the homomorphism properties. Using the homomorphism property again we get the required result since

$$\int_0^{N\cdot\iota(P)}\omega = \sum_{i=1}^{r} n_i\int_0^{D_i}\omega.$$

□

Using the homomorphism property of integration on $J_{\mathfrak{p}}$ we get a bilinear pairing

$$J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})\times H^0(J_{\mathfrak{p}},\Omega^1)\to\mathbb{K}_{\mathfrak{p}}, \tag{1.3.14}$$

which has kernel $J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})_{\text{Torsion}}$ (see [14, Theorem 2.11]) on the left and $\{0\}$ on the right. If we denote the dual of $H^0(J_{\mathfrak{p}},\Omega^1)$ by $\mathcal{T}$ then (1.3.14) is equivalent to a homomorphism

$$\log : J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})\to\mathcal{T},$$

which is a local diffeomorphism.

Let r' denote the dimension of the closure $J(\mathbb{K})^{cl}$ inside $J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$. Chabauty's idea is based on the fact that r' is bounded above by the minimum of the genus g and the Mordell-Weil rank r of J (see [36, Lemma 4.2]). So when $r<g$ he expected that the intersection $C_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})\cap J(\mathbb{K})^{cl}$ is finite. This is what he actually proved in [11].

Theorem 1.3.27 (Chabauty)**.** *Let C be a curve of genus $g\geq 2$ over $\mathbb{Q}$ and J be its Jacobian variety. Let p be a prime, and let r' be the dimension of $J(\mathbb{Q})^{cl}$ in $J_p(\mathbb{Q}_p)$. Suppose $r'<g$. Then $C_p(\mathbb{Q}_p)\cap J(\mathbb{Q})^{cl}$ is finite.*

Then Coleman in his "Effective Chabauty" paper showed how to produce very good, and as Example 1.3.29 demonstrates sometimes sharp, bounds for the size of

$C(\mathbb{K})$. This also paved the way for a widely used technique which when combined with the Mordell-Weil sieve can usually determine $C(\mathbb{K})$, assuming one can obtain a finite index subgroup of $J(\mathbb{K})$.

Theorem 1.3.28 (Coleman). *Let $\mathfrak{p}$ be an unramified prime of $\mathbb{K}$ above a rational prime p, and C be a non-singular curve of genus g, defined over $\mathbb{K}$, with good reduction at $\mathfrak{p}$. If $2g < p$ then*

$$\#C(\mathbb{K}) \leq \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) + 2g - 2.$$

Proof. This follows from [13, Proposition 1] and [13, Corollary 4a]. □

Let $\omega_1, \ldots, \omega_g$ be a basis for $H^0(J_{\mathfrak{p}}, \Omega^1)$. When $r \leq g-1$, there exist $a_1, \ldots, a_g \in \mathbb{K}_{\mathfrak{p}}$, not all zero, such that $\omega = \sum_{i=1}^{g} a_i \omega_i$ corresponds to a functional $\lambda_\omega : \mathcal{T} \to \mathbb{K}_{\mathfrak{p}}$ which is zero on $\log\left(J(\mathbb{K})\right)^{cl}$. Then

$$\eta_\omega^+ : J_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \xrightarrow{\log} \mathcal{T} \xrightarrow{\lambda_\omega} \mathbb{K}_{\mathfrak{p}}$$

is zero on $J(\mathbb{K})^{cl}$. Let $B_{\mathfrak{p}}(P_0)$ denote $\mathrm{red}_{\mathfrak{p}}^{-1}(\mathrm{red}_{\mathfrak{p}}(P_0))$. If there exists $P \in B_{\mathfrak{p}}(P_0) \cap C(\mathbb{K})$ for a known $P_0 \in C(\mathbb{K})$, then

$$0 = \int_0^{[P-P_0]} \omega = \int_{P_0}^{P} \iota^* \omega = I\left(\tau(P)\right),$$

where τ is a uniformizer at P_0. We can bound the number of such P by bounding the number of zeros the powerseries $I \in \mathrm{PS}_{\mathfrak{p}}(1,1)$ can have on $\mathcal{B}_{\mathfrak{p}}(1,1)$ using Lemma 1.3.23.

Example 1.3.29. Let C be the genus 2, hyperelliptic, plane curve with affine patch defined by the equation

$$y^2 = x^5 + 5x^4 + 8x + 4. \tag{1.3.15}$$

After searching we find the following rational points:

$$H^{\mathrm{search}} = \{\infty, (-1,0), (0,-2), (0,2), (-2,-6), (-2,6), (3,-26), (3,26)\} \subseteq C(\mathbb{Q}).$$

Using MAGMA [4] we computed that $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ with the free part generated by the divisor class $D = [(0,-2) + (-2,6) - 2\infty]$. We will perform the argument using the prime $p = 5$. We find that over $\mathbb{F}_5$ the curve has the following points:

$$\overline{C}_5(\mathbb{F}_5) = \{\infty, (0,3), (0,2), (3,1), (3,4), (4,0)\}.$$

At this point we could just use Theorem 1.3.28 and conclude that $H^{\text{search}} = C(\mathbb{Q})$, but for the sake of demonstrating how Coleman's argument works in practice on each individual residue class, we will carry on the computation.

Let $\omega_1, \omega_2 \in H^0(J_{\mathbb{Q}_5}, \Omega^1)$ be such that $\iota^*\omega_1 = dx/y$ and $\iota^*\omega_2 = xdx/y$. Then $\{\omega_1, \omega_2\}$ is a basis for $H^0(J_{\mathbb{Q}_5}, \Omega^1)$. We observe that the points $(-2,-6)$ and $(3,-26)$ reduce to the same point modulo 5. This will make our calculation slightly easier because $13D = [(3,-26) - (-2,-6)] \in J(\mathbb{Q})$ is already in the residue class of the identity. We want to find an ω such that $\eta_\omega^+(D) = 0$. This is equivalent to finding an $a \in \mathbb{Q}_5$ such that

$$0 = \int_{(-2,-6)}^{(3,-26)} \frac{(1+ax)dx}{y} = \int_{(-2,-6)}^{(3,-26)} \frac{dx}{y} \; + \; a \int_{(-2,-6)}^{(3,-26)} \frac{xdx}{y}.$$

We use $\tau = x + 2$ as a uniformizing parameter to expand:

$$\begin{aligned} I_1 = \int_{(-2,-6)}^{(3,-26)} \frac{dx}{y} &= \int_0^5 \left(-\frac{1}{6} - \frac{1}{6}\tau - \frac{17}{108}\tau^2 - \frac{5}{36}\tau^3 - \frac{10}{81}\tau^4 + \dots \right) d\tau \\ &= -1 \times 5 - 2 \times 5^2 + 2 \times 5^3 + 5^4 + O(5^5), \end{aligned}$$

$$\begin{aligned} I_2 = \int_{(-2,-6)}^{(3,-26)} \frac{xdx}{y} &= \int_0^5 \left(\frac{1}{3} + \frac{1}{6}\tau + \frac{4}{27}\tau^2 + \frac{13}{108}\tau^3 + \frac{35}{324}\tau^4 + \dots \right) d\tau \\ &= 2 \times 5 + 5^2 + 5^4 + O(5^5). \end{aligned}$$

So we must have

$$a = -\frac{I_1}{I_2} = -2 + 2 \times 5^2 + O(5^4).$$

So setting $\omega = \omega_1 + a\omega_2$ and using Lemma 1.3.23 to bound the zeros its antiderivative has on the residue class of each point in $\overline{C}_5(\mathbb{F}_5)$, as shown in Table 1.1, we see that all the elements of $C(\mathbb{Q})$ are accounted for in H^{search}. We only had to check six of them, because the other two lie in some residue class already on the table.

$P_0 \in H'$	$\text{red}_5(P_0)$	uniformizer τ	$\omega = (\ldots)d\tau$	$\#B_5(P_0) \leq$
∞	∞	y/x^3	$(-1 + O(5)) + O(\tau)$	1
$(-1, 0)$	$(4, 0)$	y	$(2 + O(5)) + O(\tau)$	1
$(0, -2)$	$(0, 3)$	x	$(2 + O(5)) + O(\tau)$	1
$(0, 2)$	$(0, 2)$	x	$(-2 + O(5)) + O(\tau)$	1
$(-2, -6)$	$(3, 4)$	$x + 2$	$(O(5)) + (2 + O(5))\,\tau + O(\tau^2)$	2
$(-2, 6)$	$(3, 1)$	$x + 2$	$(O(5)) + (-2 + O(5))\,\tau + O(\tau^2)$	2

Table 1.1: Performing Chabauty using Lemma 1.3.23

$\boxtimes$

In the rest of this section we present another, almost equivalent[8], description of applying Chabauty-Coleman's method in practice. By avoiding the use of Lemma 1.3.23, which is based on the theory of Newton polygons, and instead only employing tools from linear algebra to bound zeros on residue classes, this viewpoint becomes more straightforward to generalize later in Chapter 3. This was also used by Siksek in [48].

One must first make sure that the prime $\mathfrak{p}$ is chosen such that $\text{red}_\mathfrak{p} : C_\mathfrak{p}(\mathbb{K}_\mathfrak{p}) \to \overline{C}_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$ is injective when restricted to H^{search}, in other words

$$P_0, P_0' \in H^{\text{search}}, P_0 \neq P_0' \Rightarrow \text{red}_\mathfrak{p}(P_0) \neq \text{red}_\mathfrak{p}(P_0'). \tag{1.3.16}$$

Lemma 1.3.30. *Let $\mathfrak{p}$ be an unramified prime of $\mathbb{K}$ lying above an odd rational prime p. Fix a $P_0 \in C_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$. Suppose $P \in B_\mathfrak{p}(P_0) = \text{red}_\mathfrak{p}^{-1}(\text{red}_\mathfrak{p}(P_0))$. Let $\omega \in H^0(C_{\mathbb{K}_\mathfrak{p}}, \Omega^1)$*

[8] This is actually slightly weaker since primes failing property (1.3.16) cannot be used. The two descriptions are equivalent for primes satisfying this property.

such that $\overline{\omega} \in H^0(C_{\mathbb{F}_\mathfrak{p}}, \Omega^1) \setminus \{0\}$ *and* τ *be a uniformizer at* P_0*. Then*

$$\int_{P_0}^{P} \omega = \alpha\tau(P) + \beta\tau(P)^2,$$

where $\alpha, \beta \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ *with* α *being independent of* P*.*

Proof. See for example [48, Lemma 3.2]. □

Now fix a $P_0 \in H^{\text{search}}$ and let $\mathfrak{p}$ be a prime of good reduction for C and J satisfying (1.3.16). Let $\iota : C \to J$ be the Abel-Jacobi embedding with basepoint P_0 and $P \in B_\mathfrak{p}(P_0) \cap C(\mathbb{K})$ be a rational point such that $N \cdot \iota(P) = \sum_{i=1}^{r} n_i D_i$ for $N, n_1, \ldots, n_r \in \mathbb{Z}$, $N \neq 0$, $\langle D_1, \ldots, D_r \rangle$ a finite index subgroup of $J(\mathbb{K})$. Let $\omega_1, \ldots, \omega_g$ be a basis for $H^0(J_{\mathbb{K}_\mathfrak{p}}, \Omega^1)$. Then by Corollary 1.3.26 and Lemma 1.3.30, we can obtain $\alpha_i, \beta_i \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$, for each $1 \leq i \leq g$, such that α_i is independent of P and the following equality holds:

$$\sum_{j=1}^{r} \frac{n_j}{N} \int_0^{D_j} \omega_i = \alpha_i\tau(P) + \beta_i\tau(P)^2.$$

We thus get the following system of equations:

$$\underbrace{\begin{pmatrix} \int_0^{D_1} \omega_1 & \cdots & \int_0^{D_r} \omega_1 \\ \vdots & \vdots & \vdots \\ \int_0^{D_1} \omega_g & \cdots & \int_0^{D_r} \omega_g \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} n_1/N \\ \vdots \\ n_r/N \end{pmatrix}}_{\mathbf{n}} = \tau(P) \underbrace{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_g \end{pmatrix}}_{\mathbf{a}} + \tau(P)^2 \underbrace{\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_g \end{pmatrix}}_{\mathbf{b}}. \quad (1.3.17)$$

The following lemma is the analogue of computing the constant a in Example 1.3.29.

Lemma 1.3.31. *Let* $\hat{U}$ *be a* $(g-r) \times g$ *matrix with entries in* $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ *such that* $\hat{U} \cdot A = 0$ *and* $\mathbf{a}$ *be the vector defined in* (1.3.17)*. Then if* $\hat{U} \cdot \mathbf{a} \neq \mathbf{0}$ *modulo* $\mathfrak{p}$ *we have that* $B_\mathfrak{p}(P_0) \cap C(\mathbb{K}) = \{P_0\}$*.*

Proof. When we multiply both sides of equation (1.3.17) by $\hat{U}$ we get

$$\mathbf{0} = \hat{U} \cdot A \cdot \mathbf{n} = \tau(P)\hat{U} \cdot \mathbf{a} + \tau(P)^2 \hat{U} \cdot \mathbf{b}. \quad (1.3.18)$$

Let us suppose we have $P \in B_{\mathfrak{p}}(P_0) \cap C(\mathbb{K})$ with $P \neq P_0$. Since τ is a bijection of $B_{\mathfrak{p}}(P_0)$ with $\mathfrak{p}\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ we know that $\tau(P) \neq \tau(P_0) = 0$. Let $s = \mathrm{ord}_{\mathfrak{p}}(\tau(P))$ and let $\pi \in \mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ be a uniformizer for $\mathfrak{p}$. Then divide both sides of (1.3.18) by π^s and reduce it modulo $\mathfrak{p}$ (note that by Lemma 1.3.30 this is a system of equations defined over $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$). The term $\pi^{-s}\tau(P)^2\hat{U} \cdot \mathbf{b}$ is divisible by $\mathfrak{p}$ so it reduces to zero. Since $\pi^{-s}\tau(P)$ is non-zero modulo $\mathfrak{p}$ we must have that $\hat{U} \cdot \mathbf{a}$ is zero modulo $\mathfrak{p}$. □

The following lemma implies that computing the matrix of periods A modulo $\mathfrak{p}^{h+1}$ where

$$h = \min_{1 \leq i \leq g, 1 \leq j \leq r} \left\{ \mathrm{ord}_{\mathfrak{p}} \left(\int_0^{D_j} \omega_i \right) \right\},$$

is often sufficient to obtain $\hat{U}$ modulo $\mathfrak{p}$.

Lemma 1.3.32. *Let A be as above and $\pi \in \mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ be a uniformizer for $\mathfrak{p}$. Let h be an integer such that the entries of $A_0 = \pi^h A$ are in $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ and $\overline{A_0}$ is non-zero. Let U be a $(g-r) \times g$ matrix with entries in $\mathbb{F}_{\mathfrak{p}}$ such that $U \cdot \overline{A_0} = \mathbf{0}$. If the rank of $\overline{A_0}$ is equal to r then there exists a matrix $\hat{U}$ with entries in $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ such that $\hat{U} \cdot A = \mathbf{0}$ and $U \equiv \overline{\hat{U}}$.*

Proof. The matrix of partial derivatives at any point U of the vector space defined by $U \cdot \overline{A_0} = \mathbf{0}$ is just the block-diagonal $((g-r)g) \times ((g-r)r)$ matrix $\mathrm{Diag}(\overline{A_0}, \ldots, \overline{A_0})$ which has full rank $(g-r)r$ if and only if $\overline{A_0}$ has full rank r. The required result is now an easy consequence of a generalization of Hensel's lemma, i.e. Lemma 1.3.16, stating that for varieties $V_{\mathfrak{p}}$, non-singular points in the residue field lift to points in the local field or equivalently that the image of the reduction map $\mathrm{red}_{\mathfrak{p}} : V_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}}) \to \overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ contains the subset of non-singular points in $\overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$. For a proof of this, see for example [41, Theorem 3.5.45] or [52, Lemma 1.2.1]. □

Example 1.3.33. Let C be the curve defined by equation (1.3.15). This has good reduction at 17 and we also have that 17 satisfies (1.3.16). As before, we use $D = [(0,-2) + (-2,6) - 2\infty]$ as the generator of the free part of $J(\mathbb{Q})$. The order of $\mathrm{red}_{17}(D)$ in $\overline{J}_{17}(\mathbb{F}_{17})$ is 55. We use MAGMA to compute the quadratic polynomial with coefficients

in $\mathbb{Q}$ whose roots x_1 and x_2 satisfy

$$[(x_1, y_1) + (x_2, y_2) - 2(0, -2)] = 55D.$$

We then proceed as in [56, Section 1.9] to estimate the entries of the 2×1 matrix of periods A:

$$\int_0^D \omega_1 = \frac{1}{55}\left(\int_{(0,-2)}^{(x_1,y_1)} \frac{dx}{y} + \int_{(0,-2)}^{(x_2,y_2)} \frac{dx}{y}\right) = 8 \times 17 - 3 \times 17^2 - 8 \times 17^3 + O(17^4),$$

$$\int_0^D \omega_2 = \frac{1}{55}\left(\int_{(0,-2)}^{(x_1,y_1)} \frac{xdx}{y} + \int_{(0,-2)}^{(x_2,y_2)} \frac{xdx}{y}\right) = -7 \times 17 + 3 \times 17^2 - 5 \times 17^3 + O(17^4).$$

We observe that the reduced matrix $\overline{17^{-1}A}$ has rank 1 so by Lemma 1.3.32 we know that there exists matrix $\hat{U}$ with entries in $\mathbb{Z}_{17}$ such that $\hat{U} \cdot A$ is zero and

$$\overline{\hat{U}} = \begin{pmatrix} 7 & 8 \end{pmatrix}.$$

Since none of the entries in the final column of Table 1.2 is zero modulo 17, we can use Lemma 1.3.31 to deduce that

$$B_{17}(P_0) \cap C(\mathbb{Q}) = \{P_0\}, \quad \forall\ P_0 \in H^{\text{search}}.$$

This is not a complete proof that $H^{\text{search}} = C(\mathbb{Q})$ since $\#\overline{C}_{17}(\mathbb{F}_{17}) = 20$ and we have not yet dealt with the remaining 12 residue classes that appear to be empty. This will be carried out using the Mordell-Weil sieve in Example 1.3.34 in the following section. ⊠

$P_0 \in H^{\text{search}}$	$\text{red}_{17}(P_0)$	uniformizer τ	$\overline{\mathbf{a}}$	$\overline{\hat{U} \cdot \mathbf{a}}$
∞	∞	y/x^3	$\begin{pmatrix} 0 \\ -2 \end{pmatrix}$	$\begin{pmatrix} 1 \end{pmatrix}$
$(-1, 0)$	$(16, 0)$	y	$\begin{pmatrix} 7 \\ -7 \end{pmatrix}$	$\begin{pmatrix} -7 \end{pmatrix}$
$(0, -2)$	$(0, 15)$	x	$\begin{pmatrix} 8 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 5 \end{pmatrix}$
$(0, 2)$	$(0, 2)$	x	$\begin{pmatrix} -8 \\ 0 \end{pmatrix}$	$\begin{pmatrix} -5 \end{pmatrix}$
$(-2, -6)$	$(15, 11)$	$x + 2$	$\begin{pmatrix} -3 \\ 6 \end{pmatrix}$	$\begin{pmatrix} -7 \end{pmatrix}$
$(-2, 6)$	$(15, 6)$	$x + 2$	$\begin{pmatrix} 3 \\ -6 \end{pmatrix}$	$\begin{pmatrix} 7 \end{pmatrix}$
$(3, -26)$	$(3, 8)$	$x - 3$	$\begin{pmatrix} -2 \\ -6 \end{pmatrix}$	$\begin{pmatrix} 6 \end{pmatrix}$
$(3, 26)$	$(3, 9)$	$x - 3$	$\begin{pmatrix} 2 \\ 6 \end{pmatrix}$	$\begin{pmatrix} -6 \end{pmatrix}$

Table 1.2: Performing Chabauty using linear algebra

1.3.4 The Mordell-Weil sieve

The Mordell-Weil sieving method was introduced by Scharaschkin in his doctoral thesis [46] as a method of proving the absence of rational points on curves[9] and since then it has been used extensively for this purpose. For example, Flynn in [20] applies this to curves of genus 2 and later Bruin and Stoll in [9] apply it to more general hyperelliptic curves. This technique was also adapted to prove non-existence of rational points in individual residue classes thus, when combined with the Chabauty-Coleman argument in the previous section, provides a powerful tool used for the determination of $C(\mathbb{K})$, even when this is non-empty. A thorough investigation of the Mordell-Weil sieve along with an efficient implementation can be found in [9]. Poonen in [42] gives heuristics that support his conjecture that this method can always be used to prove that $C(\mathbb{K})$ is empty, when this is the case. In this section we give the idea behind this method and then use

[9] In the case of curves the use of the Mordell-Weil sieve to prove that $C(\mathbb{K})$ is empty is essentially equivalent to the Brauer-Manin obstruction for C, assuming the conjecture that the Tate-Shafarevich group of J is finite.

it to complete Example 1.3.33.

One can trace the philosophy of the Mordell-Weil sieve back to the Chinese Remainder Theorem, or more precisely the failure of existence of an integer solving simultaneously several congruence conditions, when these conditions are set "randomly" and fail to satisfy the criteria for applicability of the CRT. To put this into perspective, suppose we require an $n \in \mathbb{Z}$ which satisfies the congruence conditions $\{n \equiv n_i \mod M_i\}_{i=0}^{s}$. When the M_i are chosen to have many common divisors and the n_i are chosen at random, one expects that the probability of finding a common solution will decrease as s increases. Now let C, J and $\iota : C \to J$ have their usual meanings and $S = \{\mathfrak{p}_i\}_{i=0}^{s}$ be a set of primes of good reduction. For the sake of argument, suppose that $\langle D \rangle = J(\mathbb{K}) \cong \mathbb{Z}$ and that we are looking for a point $P \in C(\mathbb{K})$. For such P let n be the integer such that $\iota(P) = nD$. By using (the reduction of) ι to include the elements of $\overline{C}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$ in $\overline{J}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$ we get a congruence condition $n \equiv n_{i,\mathcal{P}} \mod \#\operatorname{red}_{\mathfrak{p}_i}(J(\mathbb{K}))$, for each $\mathcal{P} \in \overline{C}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$ such that $\iota(\mathcal{P}) \in \operatorname{red}_{\mathfrak{p}_i}(J(\mathbb{K}))$. The integer n must satisfy one of these. Evidence, for example [42, Theorem 7.2], suggests that these conditions are random. If we now suppose that $P \in \mathcal{B}_{\mathfrak{p}_0}(\mathcal{P}) = \operatorname{red}_{\mathfrak{p}_0}^{-1}(\mathcal{P})$ for a particular $\mathcal{P} \in \overline{C}_{\mathfrak{p}_0}(\mathbb{F}_{\mathfrak{p}_0})$, but the corresponding congruence leads to contradictions when combined with all possible combinations of congruences at the other primes, then this contradicts the initial assumption and we can conclude that $\mathcal{B}_{\mathfrak{p}_0}(\mathcal{P}) \cap C(\mathbb{K}) = \emptyset$.

Example 1.3.34. We now continue with Example 1.3.33 to recompute the set of $\mathbb{Q}$-rational points of the curve C defined by equation (1.3.15), using the Mordell-Weil sieve. To do that we need to show that the 12 remaining residue classes modulo 17 contain no rational points. As before we use the point $(0, -2)$ to define the embedding ι and the divisor $D = [(0, -2) + (-2, -6) - 2\infty]$ as a generator for the free part of $J(\mathbb{Q})$. Let us denote by $D^{\text{tor}} = [(-1, 0) - \infty]$ the generator for the torsion. All points $\mathcal{P}$ in the set

$$\{(1,1), (1,16), (2,8), (2,9), (5,2), (5,15), (8,2), (8,15), (12,7), (12,10)\} \subset \overline{C}_{17}(\mathbb{F}_{17})$$

satisfy $\iota(\mathcal{P}) \notin \mathrm{red}_{17}(J(\mathbb{Q}))$ so we already have $\mathcal{B}_{17}(\mathcal{P}) \cap C(\mathbb{Q}) = \emptyset$ for these. The remaining points $(10, 12)$ and $(10, 5)$ satisfy

$$\iota((10,12)) - \mathrm{red}_{17}(D^{\mathrm{tor}}) = 16\,\mathrm{red}_{17}(D) \quad \text{and}$$
$$\iota((10,5)) - \mathrm{red}_{17}(D^{\mathrm{tor}}) = 43\,\mathrm{red}_{17}(D),$$

where $\mathrm{red}_{17}(D)$ has order 55 in the finite group $\overline{J}_{17}(\mathbb{F}_{17})$. So a point $P \in C(\mathbb{Q})$, that is not already in the set H^{search} will have to satisfy $\iota(P) = D^{\mathrm{tor}} + nD$ where n is congruent to either 16 or 43 modulo 55. We now choose to work with the prime 151 because $\mathrm{red}_{151}(D)$ has order 55×34. But all points $\mathcal{P}$ in the set $\overline{C}_{151}(\mathbb{F}_{151})$ such that $\iota(\mathcal{P}) \in \mathrm{red}_{151}(J(\mathbb{Q}))$ satisfy

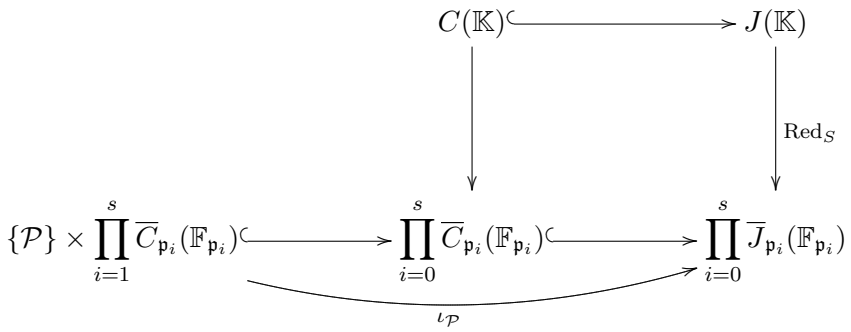
$$\iota(\mathcal{P}) - \mathrm{red}_{151}(D^{\mathrm{tor}}) = n_1\,\mathrm{red}_{151}(D),$$

where $n_1 \not\equiv 16$ and $n_1 \not\equiv 43$ modulo 55 so we cannot have an integer n such that $\iota(P) = D^{\mathrm{tor}} + nD$ for a $P \in C(\mathbb{Q})$ reducing to either $(10, 12)$ or $(10, 5)$ modulo 17, therefore both $\mathcal{B}_{17}((10, 12))$ and $\mathcal{B}_{17}((10, 5))$ contain no $\mathbb{Q}$-rational points. This completes the proof that

$$C(\mathbb{Q}) = H^{\mathrm{search}}.$$

$\boxtimes$

Let us now drop the assumption $r = 1$ to see what happens in general. Fix a point $\mathcal{P} \in \overline{C}_{\mathfrak{p}_0}(\mathbb{F}_{\mathfrak{p}_0})$ and denote by $\iota_{\mathcal{P}}$ the composition of the inclusion of $\{\mathcal{P}\} \times \prod_{i=1}^{s} \overline{C}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$ in $\prod_{i=0}^{s} \overline{C}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$, with the product of Abel-Jacobi maps over the residue fields. Also denote by Red_S the reduction map from $J(\mathbb{K})$ to the product $\prod_{i=0}^{s} \overline{J}_{\mathfrak{p}_i}(\mathbb{F}_{\mathfrak{p}_i})$. We have the following commutative diagram:



Lemma 1.3.35. *If* $\mathrm{Image}(\iota_{\mathcal{P}}) \cap \mathrm{Image}(\mathrm{Red}_S) = \emptyset$ *then* $\mathcal{B}_{\mathfrak{p}_0}(\mathcal{P}) \cap C(\mathbb{K}) = \emptyset$.

Proof. This is trivial, as a point in $\mathcal{B}_{\mathfrak{p}_0}(\mathcal{P}) \cap C(\mathbb{K})$ would map to an element in $\mathrm{Image}(\iota_{\mathcal{P}}) \cap \mathrm{Image}(\mathrm{Red}_S)$. □

A more interesting (and general) version of Lemma 1.3.35 is Theorem 3.3.1, which provides an algorithmic way to apply the Mordell-Weil sieve in practice.

Chapter 2

Descent on superelliptic curves

2.1 Preface

2.1.1 Background

When working with the set of rational points $C(\mathbb{Q})$ of an algebraic curve C, we often encounter cases, for example Selmer's curve (1.3.2), where local solubility fails to decide whether this set is empty or not. This is an important disadvantage, since local conditions are in principle easier to check than global ones. Fortunately, the method of two-cover descent on hyperelliptic curves is based on the fact that, for a hyperelliptic curve C, there is a computable collection of covers $\phi_\alpha : D_\alpha \to C$, such that

$$C(\mathbb{Q}) = \bigcup_{\alpha \in \text{finite set}} \phi_\alpha(D_\alpha(\mathbb{Q})). \tag{2.1.1}$$

Therefore, when local-to-global arguments cannot be applied directly to C, the problem can be transferred to the one of looking for rational points on the covers. This is described explicitly in [10]. In this chapter we extend this method to superelliptic curves C defined by an equation of the form $y^q = f(x)$, where q is an odd prime and $f \in \mathbb{Q}[x]$ is q-th power-free. The theory behind the process of performing descent on the Jacobian variety J of such curves, defined over a field containing the relevant roots of unity, is studied in

detail in [43]. In [15], an extension of the descent map to the Picard group of curves of this type is used to introduce new insights on the nature of $Ш(J_C/\mathbb{Q})$. Nevertheless, it is often much simpler and faster to avoid working with the rational points on the Jacobian and instead restrict to information obtained using only the initial curve. The Selmer set we define, contains information which is sometimes sufficient to determine the set $C(\mathbb{Q})$. We explain the necessary theory and present an explicit algorithm, similar to the one in [10], to compute this Selmer set. Note that we cannot use a trivial extension of the existing routines because our algorithm is expected to deal with the possibility of singular points, which do not appear in the case of hyperelliptic curves.

2.1.2 Chapter structure

In Section 2.1.3 we will present the descent map for superelliptic curves, introduce the necessary notation and explain how the information gathered after performing descent can be used to help in the determination of $C(\mathbb{Q})$.

Then, in Section 2.2 we will explain how class group and unit group information about a collection of relevant number fields is used to refine the set of interest before any local computation takes place.

The results necessary to handle the p-adic part of the computation are presented in Section 2.3, along with the corresponding algorithms. We also give the usual geometric description of the process, which is then applied to prove that the computation, in principle, terminates in finite time.

The problem of finding points on superelliptic curves generalizes the problem of finding solutions to Thue equations (see [35]) and can also be used to solve generalized Fermat equations. In Example 2.4.2 we solve four such equations considered in [27], which were used by the authors as examples of the limitations of their approach. Thus in many situations descent arguments are more appropriate than other techniques. As illustrated by Examples 2.4.1 and 2.4.2 it is often the case that C is everywhere locally soluble, but its associated covers fail to be so, preventing C from having any rational

points, since the union in (2.1.1) is comprised of empty sets. In Example 2.4.3, local information together with information obtained using subcovers, following the method of "Elliptic Curve Chabauty" proposed by Flynn and Wetherell in [21] and independently by Bruin in [5] and explored further in [6] and [7], is used to prove that the curve

$$y^3 = (x^2 - 3)(x^4 - 2)$$

has no rational points except from one rational point at ∞. By making descent applicable to singular superelliptic curves, we were able to prove in Theorem 2.4.5 that the only pair $(a, b) \in \mathbb{Z}^2_{>0}$ satisfying

$$b^3 = \sum_{i=1}^{a} i^9$$

is $(1, 1)$.

2.1.3 Setup

We have seen in 1.3.7 the definition of a superelliptic curve over a number field $\mathbb{K}$. In this chapter we will assume that our curves are defined over $\mathbb{Q}$, although the theory extends to a general number field with minor adjustments. Since the case $q = 2$ was addressed in [10], we will assume q is an odd rational prime. This will also simplify our exposition, since it will result in all curves appearing in this chapter being soluble over $\mathbb{R}$. We have also seen in Proposition 1.3.9 that any superelliptic curve (see Definition 1.3.7) can be defined by both an affine equation of the form

$$C: \quad y^q = f(x) = a_n x^n + \ldots + a_1 x + a_0$$

and the more convenient weighted homogeneous one

$$C: \quad Y^q = F(X, Z) = a_n X^n + \ldots + a_1 X Z^{n-1} + a_0 Z^n,$$

with $q \mid n$. Finally, as we have seen before, it is safe to assume that f and F are q-th power-free with integer coefficients.

We will now start using the factorizations of the polynomial f over different fields, to index various objects that will appear in this chapter. This is not a commonly used notation, but it makes the indexing more canonical. From now on let $\mathbb{L}$ denote one of $\mathbb{Q}$, $\overline{\mathbb{Q}}$, $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$ (where p can be any rational prime). Define $\mathcal{F}_{\mathbb{L}}$ to be the set of monic factors of f, that are irreducible over $\mathbb{L}$. Then

$$f = a_n \prod_{h \in \mathcal{F}_{\mathbb{L}}} h^{n_h},$$

where $1 \leq n_h \leq q-1$ for all $h \in \mathcal{F}_{\mathbb{L}}$. Denote the degree of h by d_h. Let $A_{\mathbb{L}}$ be the semi-simple $\mathbb{L}$-algebra $\mathbb{L}[x]/(f^{\mathrm{sf}}(x))$, where

$$f^{\mathrm{sf}} = \prod_{h \in \mathcal{F}_{\mathbb{L}}} h.$$

Note that f^{sf} is defined over $\mathbb{Q}$ and does not depend on $\mathbb{L}$. We denote its degree by d. $A_{\mathbb{L}}$ decomposes as a direct product of finite field extensions of $\mathbb{L}$

$$A_{\mathbb{L}} = \prod_{h \in \mathcal{F}_{\mathbb{L}}} K_h = \prod_{h \in \mathcal{F}_{\mathbb{L}}} \mathbb{L}[x]/(h(x)).$$

Denote by $\theta_h \in K_h$ the image of the generator x under the quotient map and by $\Theta_{\mathbb{L}}$ the set

$$\Theta_{\mathbb{L}} = \{\theta_h : h \in \mathcal{F}_{\mathbb{L}}\}.$$

For the following definition we will assume that a point $(X, Y, Z) \in C(\mathbb{L})$ is normalized such that if $\mathbb{L} = \mathbb{Q}$ then $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Z) = 1$ and if $\mathbb{L} = \mathbb{Q}_p$ then $X, Y, Z \in \mathbb{Z}_p$ with either $Z = 1$ or $X = 1$, $Z \in p\mathbb{Z}_p$. We can always find such representations by scaling the points.

Definition 2.1.1. For $\mathbb{L} = \mathbb{Q}$ and $\mathbb{L} = \mathbb{Q}_p$ define the component maps $\delta_h : C(\mathbb{L}) \to$

K_h^*/K_h^{*q}

$$\delta_h(X,Y,Z) = \begin{cases} (X-\theta_h Z)K_h^{*q} & \text{if } X-\theta_h Z \neq 0, \\ \sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}} & \text{otherwise,} \end{cases} \tag{2.1.2}$$

where $\widetilde{F}_h$ is the two-variable polynomial with coefficients in K_h defined by

$$(X-\theta_h Z)^{n_h}\widetilde{F}_h(X,Z) = F(X,Z) \tag{2.1.3}$$

and $\sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}}$ is defined to be the unique element $v \in K_h^*/K_h^{*q}$ such that $v^{n_h} \equiv \widetilde{F}_h(X,Z)^{-1}K_h^{*q}$. ⊠

Remark 2.1.2. (1) Note that v exists because the groups K_h^*/K_h^{*q} have exponent q and $\gcd(q,n_h)=1$ and it is unique since these groups are $\mathbb{F}_q$-vector spaces.

(2) The component maps δ_h are defined this way because for a point $(X,Y,Z) \in C(\mathbb{L})$ with $F(X,Z) \neq 0$, we have that $(X-\theta_h Z)K_h^{*q} \equiv \sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}}$, since $(X-\theta_h Z)^{n_h}\widetilde{F}_h(X,Z) = F(X,Z) = Y^q$. We also need this so that the elements α in the image of $\mu_{\mathbb{Q}}$ (see Definition 2.1.4) will be in one-to-one correspondence with a covering collection $\{\phi_\alpha : D_\alpha \to C\}$ whose elements satisfy Proposition 2.3.8.

⊠

Definition 2.1.3. Let $\delta_{\mathbb{L}} : C(\mathbb{L}) \to A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q}$ be $\delta_{\mathbb{L}} = (\delta_h)_{h\in\mathcal{F}_{\mathbb{L}}}$. ⊠

In order to account for the fact that for any $\lambda \in \mathbb{L}^*$ and $(X,Y,Z) \in C(\mathbb{L})$, $(X,Y,Z) = (\lambda X, \lambda^{n/q}Y, \lambda Z) \in C(\mathbb{L})$, we quotient the codomain of $\delta_{\mathbb{L}}$ by this action of scalars. So we define an action of $\mathbb{L}^*$ on $A_{\mathbb{L}}^*$ by

$$\lambda\,(\alpha_h)_{h\in\mathcal{F}_{\mathbb{L}}} = (\lambda\alpha_h)_{h\in\mathcal{F}_{\mathbb{L}}},$$

where $\lambda \in \mathbb{L}^*$ and $(\alpha_h)_{h\in\mathcal{F}_{\mathbb{L}}} \in A_{\mathbb{L}}^*$. This action descends to an action of $\mathbb{L}^*/\mathbb{L}^{*q}$ on $A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q}$. We denote by $A_{\mathbb{L}}^*/\mathbb{L}^*A_{\mathbb{L}}^{*q}$ the quotient of $A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q}$ by this action.

Definition 2.1.4. Define the ***descent map*** $\mu_{\mathbb{L}}$ to be the composition

$$C(\mathbb{L}) \xrightarrow{\delta_{\mathbb{L}}} A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q} \xrightarrow{\pi_{\mathbb{L}}} A_{\mathbb{L}}^*/\mathbb{L}^* A_{\mathbb{L}}^{*q}$$

where $\pi_{\mathbb{L}}$ is just the projection to the quotient. ⊠

Our aim from now on will be to obtain a finite subset of $A_{\mathbb{Q}}^*/\mathbb{Q}^* A_{\mathbb{Q}}^*$, the Selmer set, which will contain Image($\mu_{\mathbb{Q}}$) and will correspond to a finite collection of everywhere locally soluble covers of C. The rational points on these covers can help us determine the rational points on C. In particular, if the Selmer set is empty, $C(\mathbb{Q}) = \emptyset$.

2.2 Global information

2.2.1 The image of $\delta_{\mathbb{Q}}$

The image of $\delta_{\mathbb{Q}}$ is contained in a finite subgroup $A(q, \mathbf{S})$ of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$. To see this let us restrict our attention to finding the allowed possibilities for each of the $\#\mathcal{F}_{\mathbb{Q}}$ components. Let $h \in \mathcal{F}_{\mathbb{Q}}$ and set $\widetilde{f}_h(x) = f(x)/(x - \theta_h)^{n_h} \in K_h[x]$.

Suppose $(X, Y, Z) \in C(\mathbb{Q})$ with $X, Y, Z \in \mathbb{Z}$ and X coprime with Z. We have that

$$\delta_h(X, Y, Z) = (X - \theta_h Z) K_h^{*q}.$$

Now suppose that $\mathfrak{p} \nmid a_n \mathcal{O}_{K_h}$ is a prime ideal of the ring of integers $\mathcal{O}_{K_h}$ of the number field K_h. By assumption we have that

$$\mathrm{ord}_{\mathfrak{p}}(X - \theta_h Z) \geq 0, \qquad \mathrm{ord}_{\mathfrak{p}}(\widetilde{F}_h(X, Z)) \geq 0.$$

At this point we want to figure out which primes $\mathfrak{p}$ appear in the factorization of $(X - \theta_h Z)$, but not as a q-th power. So suppose $q \nmid \mathrm{ord}_{\mathfrak{p}}(X - \theta_h Z)$. Since $\gcd(n_h, q) = 1$, this implies that $q \nmid \mathrm{ord}_{\mathfrak{p}}(\widetilde{F}_h(X, Z))$. In particular we have $X \equiv \theta_h Z$ and $\widetilde{F}_h(X, Z) \equiv 0$ modulo $\mathfrak{p}$, which together give that $\widetilde{F}_h(\theta_h Z, Z) = Z^{n-n_h} \widetilde{f}_h(\theta_h) \equiv 0$ modulo $\mathfrak{p}$. But

if $Z \equiv 0$ modulo $\mathfrak{p}$ then also $X \equiv 0$ modulo $\mathfrak{p}$ which contradicts coprimality, so we have that $\mathfrak{p} \in \mathrm{Supp}(\widetilde{f}_h(\theta_h)\mathcal{O}_{K_h})$. By dropping the initial condition on $\mathfrak{p}$ we have that if $q \nmid \mathrm{ord}_{\mathfrak{p}}(X - \theta_h Z)$ then $\mathfrak{p} \in \mathrm{Supp}(a_n \widetilde{f}_h(\theta_h)\mathcal{O}_{K_h}) \subseteq \mathrm{Supp}(\Delta \mathcal{O}_{K_h})$, where $\Delta = a_n \mathrm{Disc}(f^{\mathrm{sf}})$. In other words

$$(X - \theta_h Z)\mathcal{O}_{K_h} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_l^{e_l} \mathcal{I}^q$$

where $\{\mathfrak{p}_1, \dots, \mathfrak{p}_l\} = \mathrm{Supp}\left(a_n \widetilde{f}_h(\theta_h)\mathcal{O}_{K_h}\right)$, $(e_1, \dots, e_l) \in \mathbb{F}_q^l$ and $\mathcal{I}$ is a fractional ideal of K_h.

Now define the sets of primes $S_h = \mathrm{Supp}(a_n \widetilde{f}_h(\theta_h)\mathcal{O}_{K_h})$ for $h \in \mathcal{F}_{\mathbb{Q}}$. Then by the discussion above $\mathrm{Image}(\delta_h) \subseteq K_h(q, S_h)$ where

$$K_h(q, S_h) := \{\alpha K_h^{*q} : q \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) \text{ for all } \mathfrak{p} \notin S_h\}.$$

Note that $K_h(q, S_h)$ is a finite subgroup of K_h^*/K_h^{*q} (a proof of this can be found within the proof of [50, Proposition VIII.1.6 p. 213]). Therefore we have that

$$\mathrm{Image}(\delta_{\mathbb{Q}}) \subseteq \prod_{h \in \mathcal{F}_{\mathbb{Q}}} K_h(q, S_h) =: A(q, \mathbf{S}) \tag{2.2.1}$$

which is a finite subgroup of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$.

2.2.2 The image of $\delta_{\mathbb{L}}$

Definition 2.2.1. Define the weighted norm homomorphism $\mathcal{N}_{A/\mathbb{L}} : A_{\mathbb{L}}^* \to \mathbb{L}^*$ as

$$\mathcal{N}_{A/\mathbb{L}}\left((\alpha_h)_{h \in \mathcal{F}_{\mathbb{L}}}\right) = \prod_{h \in \mathcal{F}_{\mathbb{L}}} \mathcal{N}_{K_h/\mathbb{L}}(\alpha_h)^{n_h}.$$

Since $\mathcal{N}_{A/\mathbb{L}}(A_{\mathbb{L}}^{*q})$ is a subgroup of $\mathbb{L}^{*q}$ we also get a homomorphism $\overline{\mathcal{N}}_{A/\mathbb{L}} : A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q} \to \mathbb{L}^*/\mathbb{L}^{*q}$. ⊠

Lemma 2.2.2. *We have the following inclusion:*

$$\mathrm{Image}(\delta_{\mathbb{L}}) \subseteq \mathfrak{H}_{\mathbb{L}},$$

where $\mathfrak{H}_{\mathbb{L}}$ *is defined as*

$$\mathfrak{H}_{\mathbb{L}} = \overline{\mathcal{N}}_{A/\mathbb{L}}^{-1}\left(\frac{1}{a_n}\mathbb{L}^{*q}\right).$$

Proof. By commutativity of the following diagram of norm homomorphisms

$$\begin{array}{ccc} A_{\mathbb{L}}^{*} & \xrightarrow{\mathcal{N}_{A/\mathbb{L}}} & \mathbb{L}^{*} \\ \downarrow & & \downarrow \\ A_{\mathbb{L}}^{*}/A_{\mathbb{L}}^{*q} & \xrightarrow{\overline{\mathcal{N}}_{A/\mathbb{L}}} & \mathbb{L}^{*}/\mathbb{L}^{*q} \end{array} \tag{2.2.2}$$

and the fact that

$$\prod_{h\in\mathcal{F}_{\mathbb{L}}} \mathcal{N}_{K_h/\mathbb{L}}(X-\theta_h Z)^{n_h} = Z^n \times \prod_{h\in\mathcal{F}_{\mathbb{L}}} h(X/Z)^{n_h} = \frac{Y^q}{a_n},$$

we can deduce that when $(X,Y,Z)\in C(\mathbb{L})$ satisfies $X-\theta_h Z\neq 0$ for all $h\in\mathcal{F}_{\mathbb{L}}$ we have

$$\delta_{\mathbb{L}}(X,Y,Z)\in\mathfrak{H}_{\mathbb{L}}. \tag{2.2.3}$$

So it only remains to prove (2.2.3) for $(X,Y,Z)\in C(\mathbb{L})$ with $X-\theta_{h'}Z=0$ for some $h'\in\mathcal{F}_{\mathbb{L}}$. By (2.1.2) in Definition 2.1.1, when this happens, $\delta_{h'}(X,Y,Z)=v\in K_{h'}^{*}/K_{h'}^{*q}$, where $v^{n_{h'}}=\widetilde{F}_{h'}(X,Z)^{-1}K_{h'}^{*q}$. Let $\alpha_{h'}\in K_{h'}^{*}$ be such that $\alpha_{h'}K_{h'}^{*q}=v$. Note that for $X-\theta_{h'}Z$ to be equal to zero, we must actually have $K_{h'}=\mathbb{L}$, so $\mathcal{N}_{K_{h'}/\mathbb{L}}$ is the identity and

$$\mathcal{N}_{K_{h'}/\mathbb{L}}(\alpha_{h'})^{n_{h'}}=\alpha_{h'}^{n_{h'}}=\widetilde{F}_{h'}(X,Z)^{-1}\beta_{h'}^{q}$$

for some $\beta_{h'} \in \mathbb{L}^*$. But then

$$\mathcal{N}_{K_{h'}/\mathbb{L}}(\alpha_{h'})^{n_{h'}} \prod_{h \in \mathcal{F}_{\mathbb{L}} \setminus \{h'\}} \mathcal{N}_{K_h/\mathbb{L}}(X - \theta_h Z)^{n_h} = \frac{1}{a_n} \beta_{h'}^q. \tag{2.2.4}$$

By (2.2.4) and by commutativity of diagram (2.2.2), we get that

$$\overline{\mathcal{N}}(\delta_{\mathbb{L}}(X, Y, Z)) = \frac{1}{a_n} \mathbb{L}^{*q},$$

which completes the proof. □

Note that, if non-empty, $\mathfrak{H}_{\mathbb{L}}$ is a coset of the subgroup Kernel$(\overline{\mathcal{N}}_{A/\mathbb{L}})$ in $A_{\mathbb{L}}^*/A_{\mathbb{L}}^{*q}$. Combining Lemma 2.2.2 with the inclusion (2.2.1) we deduce that

$$\text{Image}(\delta_{\mathbb{Q}}) \subseteq \mathfrak{H}_{\mathbb{Q}} \cap A(q, \mathbf{S}) =: \mathfrak{H}_{\mathbb{Q}}(\mathbf{S}).$$

2.2.3 The image of $\mu_{\mathbb{Q}}$

Lemma 2.2.3. *Let $A_{\mathbb{Q}}$ be the semi-simple $\mathbb{Q}$-algebra associated to the curve C and $A(q, \mathbf{S})$ be the subgroup of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$ defined in* (2.2.1). *Also set*

$$T := \{p \text{ prime} : \text{for all } h \in \mathcal{F}_{\mathbb{Q}}, \text{ and all } \mathfrak{p} \in \text{Supp}(p\mathcal{O}_{K_h}), (q \mid \text{ord}_{\mathfrak{p}}(p\mathcal{O}_{K_h})) \text{ or } (\mathfrak{p} \in S_h)\}.$$

Let $\iota : \mathbb{Q}^*/\mathbb{Q}^{*q} \to A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$ denote the reduction to the quotients of the inclusion $\iota : \mathbb{Q} \to A_{\mathbb{Q}}$. We have the following exact sequence:

$$\begin{array}{ccccccc} \mathbb{Q}^*/\mathbb{Q}^{*q} & \xrightarrow{\iota} & A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q} & \xrightarrow{\pi_{\mathbb{Q}}} & A_{\mathbb{Q}}^*/\mathbb{Q}^* A_{\mathbb{Q}}^{*q} & \longrightarrow & 1 \\ \uparrow & & \uparrow & \nearrow & & & \\ \mathbb{Q}(q, T) & & A(q, \mathbf{S}) & & & & \end{array}$$

Then

(i) $\text{Image}(\iota) \cap A(q, \mathbf{S}) = \iota(\mathbb{Q}(q, T))$

(ii) $\pi_{\mathbb{Q}}\left(A(q,\mathbf{S})\right) \cong A(q,\mathbf{S})/\iota\left(\mathbb{Q}(q,T)\right)$.

Proof. (i) First suppose that $aA^{*q} \in \iota\left(\mathbb{Q}(q,T)\right)$. Then $q \mid \mathrm{ord}_p(a)$ for all $p \notin T$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_{K_h}$ for some h, with $\mathfrak{p} \notin S_h$. We know that

$$\mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_{K_h}) = \mathrm{ord}_{\mathfrak{p}}(p\mathcal{O}_{K_h}) \times \mathrm{ord}_p(a),$$

so by the definition of T at least one of the factors will be divisible by q thus also their product, which implies that $aA^{*q} \in A(q,\mathbf{S})$.

For the opposite inclusion, suppose that $a \in \mathbb{Q}^*$ and $aA^{*q} \in A(q,\mathbf{S})$. Then $q \mid \mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_{K_h})$ for all $h \in \mathcal{F}_{\mathbb{Q}}$ and for all $\mathfrak{p} \notin S_h$ so if $p \notin T$, then q must divide $\mathrm{ord}_p(a)$ since q divides the product but not the first factor in the equality above.

(ii) We have

$$\pi_{\mathbb{Q}}\left(A(q,\mathbf{S})\right) \cong \frac{A(q,\mathbf{S})}{\mathrm{Kernel}(\pi_{\mathbb{Q}}) \cap A(q,\mathbf{S})} = \frac{A(q,\mathbf{S})}{\mathrm{Image}(\iota) \cap A(q,\mathbf{S})} \overset{(i)}{=} \frac{A(q,\mathbf{S})}{\iota\left(\mathbb{Q}(q,T)\right)}.$$

□

Let us denote $\pi_{\mathbb{L}}(\mathfrak{H}_{\mathbb{L}})$ by $\overline{\mathfrak{H}}_{\mathbb{L}}$ and when $\mathbb{L} = \mathbb{Q}$ let us denote $\pi_{\mathbb{Q}}(\mathfrak{H}_{\mathbb{Q}}(\mathbf{S}))$ by $\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$. Since $\mathrm{Image}(\delta_{\mathbb{Q}}) \subseteq \mathfrak{H}_{\mathbb{Q}}(\mathbf{S})$, we have that

$$\mathrm{Image}(\mu_{\mathbb{Q}}) \subseteq \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}). \tag{2.2.5}$$

In the following section we will see how $\mathrm{Image}(\mu_{\mathbb{Q}})$ is contained in a potentially strict subset of $\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$ and provide an algorithm to compute it.

2.3 Local information

2.3.1 Determining the image of $\mu_{\mathbb{Q}_p}$

In this section we will provide an algorithm which determines $\text{Image}(\mu_{\mathbb{Q}_p})$ for a rational prime p. The algorithm relies on the fact that points on C which lie in a "sufficiently small" p-adic neighborhood, have the same image under $\mu_{\mathbb{Q}_p}$.

The diagram below is crucial in the process of refining the possible image of $\mu_{\mathbb{Q}}$ even further:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\mu_{\mathbb{Q}}} & A^*_{\mathbb{Q}}/\mathbb{Q}^* A^{*q}_{\mathbb{Q}} \\ {\scriptstyle \iota_p}\downarrow & & \downarrow{\scriptstyle r_p} \\ C(\mathbb{Q}_p) & \xrightarrow{\mu_{\mathbb{Q}_p}} & A^*_{\mathbb{Q}_p}/\mathbb{Q}_p^* A^{*q}_{\mathbb{Q}_p} \end{array}$$

By commutativity, if we have a rational point $P \in C(\mathbb{Q})$ then $\mu_{\mathbb{Q}_p} \circ \iota_p(P) = r_p \circ \mu_{\mathbb{Q}}(P)$. Therefore we have that

$$\text{Image}(\mu_{\mathbb{Q}}) \subseteq r_p^{-1}(\text{Image}(\mu_{\mathbb{Q}_p})) \cap \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) \tag{2.3.1}$$

Definition 2.3.1. The **Selmer set** over $\mathbb{Q}$ of the superelliptic curve C, is defined as

$$\text{Sel}^{(\mu)}(C, \mathbb{Q}) = \left\{ [\alpha] \in \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) : r_p([\alpha]) \in \text{Image}(\mu_{\mathbb{Q}_p}) \text{ for all rational primes } p \right\}.$$

⊠

Remark 2.3.2. Strictly speaking, the set defined here corresponds to the "fake" Selmer set found generally in the literature (e.g. [10] and [15]). Roughly, the difference between the fake and the actual Selmer set is that the latter distinguishes between covers (defined in Section 2.3.2) $\phi_\alpha : D_\alpha \to C$ and $\phi_{\alpha'} : D_{\alpha'} \to C$ when ϕ_α and $\phi_{\alpha'}$ are different even if D_α and $D_{\alpha'}$ are isomorphic. Since we are not using both sets, we omit the "fake" from the notation. ⊠

After considering the inclusion (2.2.5) in the end of Section 2.2.3 and the inclusions

(2.3.1) for every rational prime p we get that

$$\text{Image}(\mu_{\mathbb{Q}}) \subseteq \text{Sel}^{(\mu)}(C, \mathbb{Q}).$$

Let $h \in \mathcal{F}_{\mathbb{Q}_p}$ and denote by $\mathfrak{p}_h$ the prime of $\mathcal{O}_{K_h}$. The following two lemmas are used to show that the analytic space $C(\mathbb{Q}_p)$ can be covered by a finite number of neighborhoods, where the map $\mu_{\mathbb{Q}_p}$ is constant. In practice X_k (or X) will be a finite precision approximation to the first coordinate of a point $(X', Y', 1) \in C(\mathbb{Q}_p)$.

Lemma 2.3.3. *Suppose that $X', X_k \in \mathbb{Z}_p$ with $\text{ord}_p(X' - X_k) \geq k$*

(i) If $k \geq \frac{2\,\text{ord}_{\mathfrak{p}_h}(q)+\text{ord}_{\mathfrak{p}_h}(X_k-\theta_h)+1}{e_{\mathfrak{p}_h/p}}$ then $(X_k - \theta_h)K_h^{*q} = (X' - \theta_h)K_h^{*q}$.

(ii) If $k \geq \frac{2\,\text{ord}_{\mathfrak{p}_h}(q)+\text{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k))+1}{e_{\mathfrak{p}_h/p}}$ then $\widetilde{f}_h(X_k)K_h^{*q} = \widetilde{f}_h(X')K_h^{*q}$.

Proof. (i) By the assumption $X' = X_k + up^k$ where $u \in \mathbb{Z}_p$. So

$$\frac{X' - \theta_h}{X_k - \theta_h} = 1 + \frac{up^k}{X_k - \theta_h}.$$

Now let $\tau(t) = \frac{X'-\theta_h}{X_k-\theta_h} - t^q$. By Hensel's lemma we have that the following is a sufficient condition for τ to have a solution in K_h,

$$\text{ord}_{\mathfrak{p}_h}(\tau(1)) \geq 2\,\text{ord}_{\mathfrak{p}_h}\left(\frac{d\tau}{dt}(1)\right) + 1,$$

or equivalently

$$k\,\text{ord}_{\mathfrak{p}_h}(p) - \text{ord}_{\mathfrak{p}_h}(X_k - \theta_h) \geq 2\,\text{ord}_{\mathfrak{p}_h}(q) + 1.$$

So, as long as the condition of the lemma is satisfied Hensel's lemma ensures that $(X_k - \theta_h)$ and $(X' - \theta_h)$ are the same modulo K_h^{*q}.

(ii) This is very similar to the previous part. Just use the fact that $\widetilde{f}_h(X') = \widetilde{f}_h(X_k + up^k) = \widetilde{f}_h(X_k) + vp^k$ where $v \in \mathbb{Z}_p$ and set $\tau(t) = \frac{\widetilde{f}_h(X')}{\widetilde{f}_h(X_k)} - t^q$.

□

Lemma 2.3.4. *If* $\{X_k\}_{k=1}^{\infty} \subset \mathbb{Z}_p$ *is a sequence satisfying* $\mathrm{ord}_p(X' - X_k) \geq k$ *for some* $X' \in \mathbb{Z}_p$ *and every* k*, then there exists* $N \in \mathbb{Z}_{>0}$ *such that* X_N *satisfies at least one of conditions (i) or (ii) of Lemma 2.3.3.*

Proof. Suppose such N does not exist. This means that for every k we have

$$\min\left\{\frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(X_k - \theta_h) + 1}{e_{\mathfrak{p}_h/p}}, \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k)) + 1}{e_{\mathfrak{p}_h/p}}\right\} > k$$

and therefore both $\mathrm{ord}_{\mathfrak{p}_h}(X_k - \theta_h)$ and $\mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k))$ tend to infinity as k tends to infinity. But since $\{X_k\}_{k=1}^{\infty}$ converges to X' we have that $(X' - \theta_h) = \widetilde{f}_h(X') = 0$, a contradiction. □

A clear distinction between the case of hyperelliptic ($q = 2$) and superelliptic ($q > 2$) curves is that, a superelliptic curve is allowed to have singularities, since f being q-th power-free is no longer equivalent to f not having repeated roots. At this point we would like to use some version of Hensel's lemma to determine whether our finite precision X_k lifts to $\mathbb{Z}_p$ as the first coordinate of a point $(X', Y', 1) \in C(\mathbb{Q}_p)$. We have to be careful not to ask this question for points approximating one of the singularities as that would result in an infinite loop. Thus we have to determine the size of the $\mu_{\mathbb{Q}_p}$-constant neighborhood around each singularity (which is defined over $\mathbb{Q}_p$) in advance and compute its image.

Let

$$\mathcal{F}_{\mathbb{Q}_p}^{lsi} = \left\{h \in \mathcal{F}_{\mathbb{Q}_p} : \deg(h) = 1, n_h > 1, \theta_h \in \mathbb{Z}_p\right\},$$

where the exponent *lsi* stands for linear, singular and integral. Elements of this set correspond to the singular points on C that are defined over $\mathbb{Q}_p$, but are of the form $(\theta_h, 0, 1)$ with $\theta_h \in \mathbb{Z}_p$. The last condition arises because we split the computation into two parts, the first being the determination of the image under $\mu_{\mathbb{Q}_p}$ of points of the form

$(X', Y', 1) \in C(\mathbb{Q}_p)$, with $X', Y' \in \mathbb{Z}_p$.

Algorithm 1 The SizeOfNeighborhood function

1: **function** SizeOfNeighborhood(h)
2: $k_h \leftarrow 0$
3: Finish $\leftarrow$ **false**
4: **while** [Finish = **false**] **do**
5: $k_h \leftarrow k_h + 1$
6: $X \leftarrow X \in \mathbb{Z} \subset \mathbb{Z}_p : \mathrm{ord}_{\mathfrak{p}_h}(X - \theta_h) \geq k_h$
7: ValList$\leftarrow$ $\left\{ \frac{2\,\mathrm{ord}_{\mathfrak{p}_{h'}}(q) + \mathrm{ord}_{\mathfrak{p}_{h'}}(X - \theta_{h'}) + 1}{e_{\mathfrak{p}_{h'}/p}} : h' \in \mathcal{F}_{\mathbb{Q}_p} \setminus \{h\} \right\} \cup \left\{ 2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X)) + 1 \right\}$
8: **if** [$\max($ValList$) \leq k_h$] **then**
9: Finish $\leftarrow$ **true**
10: **end if**
11: **end while**
12: **return** k_h, X
13: **end function**

Note that the function SizeOfNeighborhood (Algorithm 1) only makes sense when $\deg(h) = 1$ otherwise we would not be able to find an X satisfying the condition of step 6 for every given k_h (that would imply that $\theta_h \in \mathbb{Z}_p$), and we will actually only apply it to elements of $\mathcal{F}^{lsi}_{\mathbb{Q}_p}$. This function has a double use: The returned value of X will be used to compute $\mu_{\mathbb{Q}_p}(\theta_h, 0, 1)$, and k_h will keep track of the size of the $\mu_{\mathbb{Q}_p}$-constant neighborhood around the singularity. Now for $h \in \mathcal{F}^{lsi}_{\mathbb{Q}_p}$ set

$$\mathcal{U}_h = \{X \in \mathbb{Z}_p : \mathrm{ord}_p(X - \theta_h) \geq k_h\}$$

and

$$\mathcal{U} = \bigcup_{h \in \mathcal{F}^{lsi}_{\mathbb{Q}_p}} \mathcal{U}_h.$$

The following function can be thought of as partitioning $\mathbb{Z}_p$ into neighborhoods, with the partition becoming finer close to the singularities. Then the function LocalImage (Algorithm 3) will test each of these neighborhoods for elements that lift to points

on C, and if necessary partition them further into $\mu_{\mathbb{Q}_p}$-constant parts.

Algorithm 2 The ComputeInputList function

```
1: function ComputeInputList(Reps, k, List)
2:     for X ∈ Reps do
3:         NeedRecursion←false
4:         for h ∈ F^{lsi}_{Q_p} do
5:             if k_h > k and ord_p(X − θ_h) ≥ k_h then
6:                 NeedRecursion← true
7:             end if
8:         end for
9:         if NeedRecursion then
10:            List ←ComputeInputList({X + tp^k : t ∈ {0, ..., p − 1}}, k + 1, List)
11:        else
12:            List ← List ∪{(X, k)}
13:        end if
14:    end for
15:    return List
16: end function
```

At this point we should stress that the functions SizeOfNeighborhood (Algorithm 1) and ComputeInputList (Algorithm 2) would be redundant if there were no singularities, and the function LocalImage (Algorithm 3) would be sufficient to compute the local image. In that case the input (List=$\{0,\ldots,p-1\}$,Image=$\{\}$) would produce the require result.

With the help of the SizeOfNeighborhood function, we pre-compute and store in the variable *image* the images of the singular points under $\mu_{\mathbb{Q}_p}$. Using LocalImage (Algorithm 3) with initial input

$$(\text{ComputeInputList}\,(\{0,\ldots,p-1\},1,\{\})\,,\text{image})$$

we get as output a set $V_1 \subseteq A^*_{\mathbb{Q}_p}/\mathbb{Q}^*_p A^{*q}_{\mathbb{Q}_p}$ which satisfies $\mu_{\mathbb{Q}_p}(U_1) = V_1$, where $U_1 = \{(X,Y,1) \in C(\mathbb{Q}_p) : X, Y \in \mathbb{Z}_p\}$. With slight modifications to the routine above we can also obtain as output a set V_2 such that $\mu_{\mathbb{Q}_p}(U_2) = V_2$, where $U_2 = \{(1,Y,pZ) \in C(\mathbb{Q}_p) : Y, Z \in \mathbb{Z}_p\}$. Thus we obtain the complete image of $\mu_{\mathbb{Q}_p}$, since $U_1 \cup U_2 = C(\mathbb{Q}_p)$.

Algorithm 3 The LocalImage function

1: **function** LocalImage(List, Image)
2: **for** [$(X,k) \in$ List] **do**
3: **if** [$X \in \mathcal{U}$ **or** $\nexists (X',Y',1) \in C(\mathbb{Q}_p) : \mathrm{ord}_p(X'-X) \geq k$] **then**
4: List $\leftarrow$ List$\backslash\{(X,k)\}$
5: **else**
6: ValList$\leftarrow \left\{ \left[\frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q)+\mathrm{ord}_{\mathfrak{p}_h}(X-\theta_h)+1}{e_{\mathfrak{p}_h/p}}, \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q)+\mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X))+1}{e_{\mathfrak{p}_h/p}} \right] : h \in \mathcal{F}_{\mathbb{Q}_p} \right\}$
7: **if** [$\forall [k_1,k_2] \in$ValList, $\min(k_1,k_2) \leq k$] **then**
8: NewElement $\leftarrow 1$
9: **for** [$[k_1,k_2] \in$ValList] **do**
10: **if** [$k_1 \leq k_2$] **then**
11: NewElement $\leftarrow$ NewElement$\times (X-\theta_h)K_h^{*q}$
12: **else**
13: NewElement$\leftarrow$ NewElement $\times \sqrt[n_h]{\widetilde{f}_h(X)^{-1}K_h^{*q}}$
14: **end if**
15: **end for**
16: NewElement$\leftarrow$ $\pi_{\mathbb{Q}_p}$(NewElement)
17: Image $\leftarrow$ Image $\cup\{$NewElement$\}$
18: **else**
19: NewList$\leftarrow \{(X+tp^k, k+1) : t \in \{0,\ldots,p-1\}\}$
20: Image$\leftarrow$LocalImage(NewList, Image)
21: **end if**
22: **end if**
23: **end for**
24: **return** Image
25: **end function**

Remark 2.3.5. We can be certain that the routine LocalImage (Algorithm 3) terminates after a finite number of steps because of Lemma 2.3.4. An infinite loop would correspond to a sequence $\{X_k\}_{k=1}^{\infty}$ converging to some $X' \in \mathbb{Z}_p$ satisfying $X' - \theta_h = \widetilde{f}_h(X') = 0$ which is impossible. Also note that the If statement at step 3, ensures that if $X \in \mathcal{U}$, in other words if our approximate value is very close to the first coordinate of one of the singular points, then it is excluded from LIST and we do not try to lift it using Hensel's Lemma, which would have resulted in an infinite loop. ⊠

2.3.2 The corresponding covers

For every $\alpha \in A_{\mathbb{L}}^*$ such that $[\alpha] := \alpha \mathbb{L}^* A^{*q} \in \overline{\mathfrak{H}}_{\mathbb{L}}$ we can construct a cover of C of degree q^{d-2}

$$\phi_\alpha : D_\alpha \to C,$$

defined over $\mathbb{L}$ satisfying the properties

$$\begin{aligned} D_\alpha(\mathbb{L}) \neq \emptyset \quad &\Leftrightarrow \quad [\alpha] \in \mathrm{Image}(\mu_{\mathbb{L}}) \\ [\alpha] = \left[\alpha'\right] \quad &\Rightarrow \quad D_\alpha \cong D_{\alpha'} \end{aligned}$$

First let us give an equivalent description of the $\mathbb{L}$-algebra $A_{\mathbb{L}}$. Denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{L}}/\mathbb{L})$ by $\mathcal{G}_{\mathbb{L}}$. We fix embeddings $K_h \hookrightarrow \overline{\mathbb{L}}$ for all $h \in \mathcal{F}_{\mathbb{L}}$ that are compatible in the sense that they agree on the intersections $K_h \cap K_{h'}$ for $h, h' \in \mathcal{F}_{\mathbb{L}}$. We then get an inclusion $\Theta_{\mathbb{L}} \hookrightarrow \Theta_{\overline{\mathbb{L}}}$ and we can treat elements $\alpha_h \in K_h$ as elements of $\overline{\mathbb{L}}$ and elements of $\Theta_{\mathbb{L}}$ as elements of $\Theta_{\overline{\mathbb{L}}}$.

Lemma 2.3.6.

$$A_{\mathbb{L}} \cong \mathrm{Map}_{\mathbb{L}}(\Theta_{\overline{\mathbb{L}}}, \overline{\mathbb{L}}),$$

where the right hand side is the set of all $\mathcal{G}_{\mathbb{L}}$-equivariant maps from $\Theta_{\overline{\mathbb{L}}}$ to $\overline{\mathbb{L}}$.

Proof. The isomorphism is given by

$$(\alpha_h)_{h\in\mathcal{F}_{\mathbb{L}}} \mapsto (\theta_{h'} \mapsto {}^{\sigma}\alpha_h : \sigma \in \mathcal{G}_{\mathbb{L}},\ h \in \mathcal{F}_{\mathbb{L}},\ {}^{\sigma}\theta_h = \theta_{h'})$$

with inverse

$$\xi \mapsto (\xi(\theta_h))_{\theta_h\in\Theta_{\mathbb{L}}\subseteq\Theta_{\overline{\mathbb{L}}}}.$$

□

Let $\alpha \in A^*_{\mathbb{L}}$ such that $[\alpha] \in \overline{\mathfrak{H}}_{\mathbb{L}}$. Since $\alpha A^{*q} \in \mathfrak{H}_{\mathbb{L}}$, there exists $v \in \mathbb{L}^*$ with

$$a_n \mathcal{N}_{A/\mathbb{L}}(\alpha) = v^q. \tag{2.3.2}$$

Let D_α be the variety in $\mathbb{P}^{d-1} \times C$ defined by

$$\Big((u_h)_{h\in\mathcal{F}_{\overline{\mathbb{L}}}}, (X,Y,Z)\Big) \in D_\alpha \Leftrightarrow \exists \lambda \neq 0 \text{ s.t. } \lambda\alpha(\theta_h)u_h^q = X - \theta_h Z \tag{2.3.3}$$
$$\text{for all } h \in \mathcal{F}_{\overline{\mathbb{L}}} \text{ and}$$
$$\lambda^{n/q} v \prod_{h\in\mathcal{F}_{\overline{\mathbb{L}}}} u_h^{n_h} = Y.$$

We use a description of the covers D_α similar, at least in terms of their ambient space, to the one found in [15] and [49]. We equip the first factor, $\mathbb{P}^{d-1}$, with the twisted $\mathcal{G}_{\mathbb{L}}$-action which permutes coordinates in the same way it permutes $\Theta_{\overline{\mathbb{L}}}$. In other words if $\sigma \in \mathcal{G}_{\mathbb{L}}$ satisfies ${}^{\sigma}\theta_h = \theta_{h'}$, then ${}^{\sigma}u_h = u_{h'}$. Another way to think of this is that we have the usual affine space $\mathbb{A}^d$ obtained as

$$\mathbb{A}^d = \operatorname{Spec}\left(\overline{\mathbb{L}}\left[\{x_{h,i}\}_{h\in\mathcal{F}_{\mathbb{L}},0\leq i\leq d_h}\right]\right)$$

and setting

$$u_h = x_{h,0} + x_{h,1}\theta_h + \ldots + x_{h,d_h-1}\theta_h^{d_h-1}$$

and then using as generators the u_h and their conjugates instead. We then take the usual quotient of $\mathbb{A}^d \setminus \{0\}$ by the action of scalars to obtain our $\mathbb{P}^{d-1}$. It is then obvious from the definition that D_α is actually defined over $\mathbb{L}$. Projection to the second factor gives rise to the required covering map

$$\phi_\alpha : D_\alpha \to C.$$

Lemma 2.3.7. *For every $P \in C(\overline{\mathbb{L}})$*

$$\#\phi_\alpha^{-1}(P) = q^{d-2}. \tag{2.3.4}$$

In particular D_α is a curve.

Proof. Let $P = (X, Y, Z) \in C(\overline{\mathbb{L}})$ and suppose $X - \theta_{h_0} Z \neq 0$ for some $h_0 \in \mathcal{F}_{\overline{\mathbb{L}}}$. Then $u_{h_0} \neq 0$ so we can set $u_{h_0} = 1$. By doing this we also fixed $\lambda = \frac{X - \theta_{h_0} Z}{\alpha(\theta_{h_0})}$. So for all u_h with $h \neq h_0$ we have

$$u_h^q = \frac{\alpha(\theta_{h_0})(X - \theta_h Z)}{\alpha(\theta_h)(X - \theta_{h_0} Z)}.$$

Since we are over $\overline{\mathbb{L}}$, if there does not exist $h \in \mathcal{F}_{\overline{\mathbb{L}}}$ such that $X - \theta_h Z = 0$, then there are exactly q different choices for the value of each of the $d-1$ u_h's. Once $d-2$ of them have been chosen, the remaining one is decided by the relation

$$\lambda^{n/q} v \prod_{h \in \mathcal{F}_{\overline{\mathbb{L}}}} u_h^{n_h} = Y.$$

The fact that there is a unique choice for the value of the remaining coordinate uses that $\gcd(n_h, q) = 1$ for every $h \in \mathcal{F}_{\overline{\mathbb{L}}}$. On the other hand if $X - \theta_{h'} Z = 0$ for some $h' \in \mathcal{F}_{\overline{\mathbb{L}}} \setminus \{h_0\}$ then $u_{h'} = 0$ and there are q choices for the remaining $d-2$ u_h's. The extra relation in this case does not decide the value for any of them. We see that in both cases the fiber of ϕ_α over $P \in C(\overline{\mathbb{L}})$ contains exactly q^{d-2} points. □

Proposition 2.3.8. *$D_\alpha(\mathbb{L}) \neq \emptyset$ if and only if $[\alpha] \in \text{Image}(\mu_{\mathbb{L}})$. Furthermore, if $[\alpha] = [\alpha']$ then $D_\alpha \cong D_{\alpha'}$ over $\mathbb{L}$. In other words, up to $\mathbb{L}$-isomorphism, D_α only depends on the class $[\alpha]$ in $A^*_{\mathbb{L}}/\mathbb{L}^* A^{*q}_{\mathbb{L}}$.*

Proof. Let $P = \Big((u_h)_{h\in\mathcal{F}_{\overline{\mathbb{L}}}}, (X,Y,Z)\Big) \in D_\alpha(\mathbb{L})$. Projecting gives $\phi_\alpha(P) = (X,Y,Z) \in C(\mathbb{L})$ and if $X - \theta_h Z \neq 0 \ \forall\ h \in \mathcal{F}_{\overline{\mathbb{L}}}$ then

$$\delta_{\mathbb{L}}\left(\phi_\alpha(P)\right) = \left((X-\theta_h Z)K_h^{*q}\right)_{\theta_h\in\Theta_{\mathbb{L}}\subseteq\Theta_{\overline{\mathbb{L}}}} = \left(\lambda\alpha_h u_h^q K_h^{*q}\right)_{\theta_h\in\Theta_{\mathbb{L}}\subseteq\Theta_{\overline{\mathbb{L}}}}$$

therefore $\mu_{\mathbb{L}}(\phi_\alpha(P)) = [\alpha]$. On the other hand if there exists $h' \in \mathcal{F}_{\overline{\mathbb{L}}}$ such that $X - \theta_{h'} Z = 0$ then

$$\begin{aligned}
\delta_{h'}(\phi_\alpha(P)) &= \sqrt[n_{h'}]{\widetilde{F}_{h'}(X,Z)^{-1} K_{h'}^{*q}} && \text{(By (2.1.2) in Definition 2.1.1)}\\
&= \sqrt[n_{h'}]{\frac{1}{a_n \prod\limits_{h\in\mathcal{F}_{\overline{\mathbb{L}}}\setminus h'} (X-\theta_h Z)^{n_h}} K_{h'}^{*q}} && \text{(By (2.1.3) in Definition 2.1.1)}\\
&= \sqrt[n_{h'}]{\frac{1}{a_n \lambda^{n-n_{h'}} \prod\limits_{h\in\mathcal{F}_{\overline{\mathbb{L}}}\setminus h'} \left(\alpha(\theta_h) u_h^q\right)^{n_h}} K_{h'}^{*q}} && \left(\begin{array}{c}\text{By (2.3.3), the defining}\\ \text{equations of the covers}\end{array}\right)\\
&= \sqrt[n_{h'}]{\frac{(\lambda\alpha_{h'})^{n_{h'}}}{a_n \lambda^n \mathcal{N}_{A/\mathbb{L}}(\alpha)} K_{h'}^{*q}} && \text{(By Definition 2.2.1)}\\
&= \sqrt[n_{h'}]{\frac{(\lambda\alpha_{h'})^{n_{h'}}}{\left(\lambda^{n/q}\upsilon\right)^q} K_{h'}^{*q}} && \text{(By (2.3.2))}\\
&= \sqrt[n_{h'}]{(\lambda\alpha_{h'})^{n_{h'}} K_{h'}^{*q}}\\
&= \lambda\alpha_{h'} K_{h'}^{*q}. && \left(\begin{array}{c}\text{By by the definition of}\\ \sqrt[n_{h'}]{\bullet} \text{ in Definition 2.1.1}\end{array}\right)
\end{aligned}$$

So again $\mu_{\mathbb{L}}(\phi_\alpha(P)) = [\alpha]$, since all the other components of $\delta_{\mathbb{L}}$ are evaluated without using cofactors.

For the other implication, suppose $[\alpha] \in \text{Image}(\mu_{\mathbb{L}})$. This means there exist

$X, Y, Z \in \mathcal{O}_{\mathbb{L}}$, $\lambda \in \mathbb{L}^*$ and $\beta \in A^*_{\mathbb{L}}$ such that

$$\lambda\alpha(\theta_h)\beta(\theta_h)^q = X - \theta_h Z$$

for $\theta_h \in \Theta_{\mathbb{L}}$. After conjugating these relations by elements of $\mathcal{G}_{\mathbb{L}}$ and using the fact that α and β are $\mathcal{G}_{\mathbb{L}}$-equivariant, we obtain the corresponding relations for $\theta_h \in \Theta_{\overline{\mathbb{L}}} \setminus \Theta_{\mathbb{L}}$. Then

$$Q = \Big((\beta(\theta_h))_{h\in\mathcal{F}_{\overline{\mathbb{L}}}}, (X, Y, Z)\Big) \in D_\alpha(\mathbb{L}). \tag{2.3.5}$$

Note that if for some $h' \in \mathcal{F}_{\mathbb{L}}$ we have $X - \theta_{h'} Z = 0$ then $d_{h'} = 1$ and the corresponding coordinate $u_{h'}$ is equal to zero.

For the last statement suppose that we have $\alpha, \alpha' \in A^*_{\mathbb{L}}$ with $[\alpha] = [\alpha']$. This implies that there exist $\lambda \in \mathbb{L}^*$ and $\beta \in A^*_{\mathbb{L}}$ such that $\alpha = \lambda\alpha'\beta^q$. By definition of the covers it is not hard to see that we can then map D_α to $D_{\alpha'}$ via $\Big((u_h)_{h\in\mathcal{F}_{\overline{\mathbb{L}}}}, (X, Y, Z)\Big) \mapsto \Big((\beta(\theta_h)u_h)_{h\in\mathcal{F}_{\overline{\mathbb{L}}}}, (X, Y, Z)\Big)$ which is clearly an isomorphism and it is defined over $\mathbb{L}$ since it is invariant under the twisted $\mathcal{G}_{\mathbb{L}}$-action. □

Corollary 2.3.9. *Let $\mathcal{H}$ be any subset of $\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$ containing* $\mathrm{Image}(\mu_{\mathbb{Q}})$*, then*

$$C(\mathbb{Q}) = \bigcup_{[\alpha]\in\mathcal{H}} \phi_\alpha\left(D_\alpha(\mathbb{Q})\right).$$

In particular the above equality holds for $\mathcal{H} = \mathrm{Sel}^{(\mu)}(C, \mathbb{Q})$.

Proof. Since for all $\alpha \in A^*_{\mathbb{Q}}$ such that $[\alpha] \in \overline{\mathfrak{H}}_{\mathbb{Q}}$, D_α and ϕ_α are defined over $\mathbb{Q}$, we know that the right hand side is contained in $C(\mathbb{Q})$. Also, from the proof of Proposition 2.3.8, in particular (2.3.5), we deduce that if we have $P = (X, Y, Z) \in C(\mathbb{Q})$ and $\mu_{\mathbb{Q}}(P) = [\alpha]$, then there exists $Q \in D_\alpha(\mathbb{Q})$ with $\phi_\alpha(Q) = P$. On the other hand, if $[\alpha] \in \mathcal{H} \setminus \mathrm{Image}(\mu_{\mathbb{Q}})$ then $D_\alpha(\mathbb{Q}) = \emptyset$. □

Proposition 2.3.10. *The curves D_α are non-singular.*

Proof. To show this let us restrict to the affine patch where $u_{h_0} \neq 0$ and $Z \neq 0$ for some $h_0 \in \mathcal{F}_{\overline{\mathbb{L}}}$. We thus assume that $u_{h_0} = Z = 1$, label the elements of $\mathcal{F}_{\overline{\mathbb{L}}} \setminus \{h_0\}$ using an index $i \in \{1, \ldots, d-1\}$ and rename $u_i := u_{h_i}$, $\theta_i := \theta_{h_i}$ and $n_i := n_{h_i}$ to simplify the notation. Thus equations (2.3.3), the defining equations for D_α, in this patch become

$$\begin{aligned} &\alpha(\theta_i)(X-\theta_0)u_i^q = \alpha(\theta_0)(X-\theta_i) && \text{for } i \in \{1,\ldots,d-1\} \\ &v\left(\frac{X-\theta_0}{\alpha(\theta_0)}\right)^{n/q} \prod_{i=1}^{d-1} u_i^{n_i} = Y. \end{aligned}$$

We get the following $(d+1) \times d$ matrix of partial derivatives which represents a linear map whose cokernel is the cotangent space of D_α at a generic point of the affine patch.

$$\begin{pmatrix} \alpha(\theta_1)u_1^q - \alpha(\theta_0) & \alpha(\theta_2)u_2^q - \alpha(\theta_0) & \ldots & \alpha(\theta_{d-1})u_{d-1}^q - \alpha(\theta_0) & v\left(\frac{n}{q}\right)\alpha(\theta_0)^{-n/q}(X-\theta_0)^{n/q-1}\prod_{i=1}^{d-1} u_i^{n_i} \\ q\alpha(\theta_1)(X-\theta_0)u_1^{q-1} & 0 & \ldots & 0 & vn_1\left(\frac{X-\theta_0}{\alpha(\theta_0)}\right)^{n/q} u_1^{n_1-1}\prod_{i\neq 0,1} u_i^{n_i} \\ 0 & q\alpha(\theta_2)(X-\theta_0)u_2^{q-1} & \ldots & 0 & vn_2\left(\frac{X-\theta_0}{\alpha(\theta_0)}\right)^{n/q} u_2^{n_2-1}\prod_{i\neq 0,2} u_i^{n_i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & q\alpha(\theta_{d-1})(X-\theta_0)u_{d-1}^{q-1} & vn_{d-1}\left(\frac{X-\theta_0}{\alpha(\theta_0)}\right)^{n/q} u_{d-1}^{n_{d-1}-1}\prod_{i\neq 0,d-1} u_i^{n_i} \\ 0 & 0 & \ldots & 0 & -1 \end{pmatrix} \tag{2.3.6}$$

This matrix has rank d at every point of the affine patch. To see this note that the first $d-1$ entries of the first row, can never be zero, since this would contradict the fact that the roots of f^{sf} are distinct. For the same reason, at most one row can be identically zero and when this happens the $d \times d$ matrix obtained by deleting that row has rank d. A similar argument for all of the $2d$ affine patches covering D_α shows that D_α is non-singular. □

Proposition 2.3.11. *Let Δ be the discriminant of the polynomial f^{sf}. If p is a rational prime such that $p \nmid q\Delta$ and $\alpha \in A^*_{\mathbb{Q}}$ such that $[\alpha] \in \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$, then D_β has good reduction, where $\beta \in A^*_{\mathbb{Q}_p}$ is such that $[\beta] = r_p([\alpha])$.*

Proof. Since p does not divide q or Δ, $\alpha \in A^*_{\mathbb{Q}}$ can be chosen such that $\mathrm{ord}_{\mathfrak{p}}(\alpha(\theta_h)) = 0$ for every $h \in \mathcal{F}_{\overline{\mathbb{Q}}}$ and every $\mathfrak{p} \mid p$. Take β to be the image of this α under the inclusion

$\otimes\mathbb{Q}_p : A^*_{\mathbb{Q}} \to A^*_{\mathbb{Q}_p}$. Then $[\beta] = r_p([\alpha])$ and also $\mathrm{ord}_{\mathfrak{p}}(\beta(\theta_h)) = 0$ for every $h \in \mathcal{F}_{\overline{\mathbb{Q}_p}}$ and every $\mathfrak{p} \mid p$. Thus the defining equation

$$\lambda\beta(\theta_h)u_h^q = X - \theta_h Z$$

of D_β can be reduced to a non-zero equation modulo $\mathfrak{p}_h$ for every $h \in \mathcal{F}_{\overline{\mathbb{Q}_p}}$, where $\mathfrak{p}_h$ is the prime of K_h above p. We thus get a cover $\overline{\phi_\beta} : \overline{D_\beta} \to \overline{C}$ defined over $\mathbb{F}_p$. Furthermore we know that $\overline{D_\beta}$ is non-singular since the reduction of the matrix of partial derivatives in (2.3.6) has full rank. □

Proposition 2.3.12. *The genus G of the covers D_α is equal to $q^{d-2}\left(\frac{d(q-1)}{2} - q\right) + 1$.*

Proof. Let $\psi : C \to \mathbb{P}^1$ be the map $(X, Y, Z) \mapsto (X, Z)$. This has degree q. Since ϕ_α has degree q^{d-2} by Lemma 2.3.7, the composition $\psi \circ \phi_\alpha : D_\alpha \to \mathbb{P}^1$, which is a non-constant morphism between two non-singular varieties, has degree q^{d-1}. It is easy to see that for every $(X, 1) \in \mathbb{P}^1$, with $X \notin \Theta_{\overline{\mathbb{L}}}$ (in other words when X is not a root of f), we have

$$\#\psi^{-1}(X, 1) = q,$$

and combining this with equation (2.3.4) we get that

$$\#(\psi \circ \phi_\alpha)^{-1}(X, 1) = q^{d-1} = \deg(\psi \circ \phi_\alpha), \forall\ X \notin \Theta_{\overline{\mathbb{L}}}.$$

By considering the affine patch where $X \neq 0$ we can show that the size of the fiber above the point $(1, 0) \in \mathbb{P}^1$ is also q^{d-1}. By Proposition 1.3.5 we deduce that for $P_{\mathrm{un}} = (X, 1)$ with $X \notin \Theta_{\overline{\mathbb{L}}}$ and $P_{\mathrm{un}} = (1, 0)$ we have

$$e_{\psi\circ\phi_\alpha}(Q) = 1 \quad \forall\ Q \in (\psi \circ \phi_\alpha)^{-1}(P_{\mathrm{un}}). \tag{2.3.7}$$

Now take $P_{\mathrm{ram}} = (\theta_h, 1) \in \mathbb{P}^1$ for some $\theta_h \in \Theta_{\overline{\mathbb{L}}}$. Then $\tau = x - \theta_h$ is a uniformizer at

P_{ram} for $\mathbb{P}^1$ and by the defining equations (2.3.3) of D_α we have that

$$(\psi \circ \phi_\alpha)^*(\tau) = x - \theta_h = (x - \theta_{h'}) \frac{\alpha(th_h)}{\alpha(th_{h'})} u_h^q,$$

for some $h' \in \mathcal{F}_{\overline{\mathbb{L}}} \setminus \{h\}$.[1] Since u_h is actually a uniformizing parameter for all points in $(\psi \circ \phi_\alpha)^{-1}(P_{\text{ram}})$, and $(x - \theta_{h'})$ is non-zero and regular at these points, we get that that

$$e_{\psi \circ \phi_\alpha}(Q) = q \quad \forall\, Q \in (\psi \circ \phi_\alpha)^{-1}(P_{\text{ram}}). \tag{2.3.8}$$

Now by substituting (2.3.7) and (2.3.8) in the Riemann-Hurwitz formula for $\psi \circ \phi_\alpha$ we get

$$\begin{aligned} 2G - 2 =& (2\,\text{Genus}(\mathbb{P}^1) - 2)\deg(\psi \circ \phi_\alpha) + \sum_{P \in \mathbb{P}^1, Q \in (\psi \circ \phi_\alpha)^{-1}(P)} (e_Q - 1) \\ 2G - 2 =& -2q^{d-1} + dq^{d-2}(q-1) \\ G =& q^{d-2}\left(\frac{d(q-1)}{2} - q\right) + 1. \end{aligned}$$

□

Definition 2.3.13. Define the set of ***useful primes*** to be

$$S_{up} := \left\{ p \text{ rational prime } : p \mid q\Delta \quad \text{or} \quad \sqrt{p} + \frac{1}{\sqrt{p}} \leq 2G \right\}.$$

⊠

Proposition 2.3.14. *Suppose that p is a rational prime and $p \notin S_{up}$. Then $\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) \subseteq r_p^{-1}\left(\text{Image}(\mu_{\mathbb{Q}_p})\right)$.*

Proof. Let $\alpha \in A_{\mathbb{Q}}^*$ such that $[\alpha] \in \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$ and $\beta \in A_{\mathbb{Q}_p}^*$ such that $[\beta] = r_p([\alpha])$. By Propositions 2.3.11 and 2.3.12 we know that $\overline{D_\beta}$ is a non-singular curve of genus G over

[1] Note that we are actually abusing notation by denoting the affine coordinate again by u_h when it is actually $u_h/u_{h'}$.

$\mathbb{F}_p$. Then by the Hasse-Weil inequality we have that $\#\overline{D_\beta}(\mathbb{F}_p) > 0$ and we can use Hensel's lemma to lift to a point in $D_\beta(\mathbb{Q}_p)$. By Proposition 2.3.8 this is equivalent to $[\beta] = r_p([\alpha]) \in \text{Image}(\mu_{\mathbb{Q}_p})$. □

Corollary 2.3.15.

$$\text{Sel}^{(\mu)}(C, \mathbb{Q}) = \{[\alpha] \in \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) : r_p([\alpha]) \in \text{Image}(\mu_{\mathbb{Q}_p}) \textit{ for all } p \in S_{up}\}$$

2.3.3 Computational efficiency

The groups $A(q, \mathbf{S})$, $\mathbb{Q}(q, T)$ and the homomorphism ι defined in Sections 2.2.1 and 2.2.3 can be computed using commands implemented by Claus Fieker in the MAGMA computer algebra system [4], so we can compute $\pi_{\mathbb{Q}}(\mathfrak{H}_{\mathbb{Q}}(\mathbf{S})) = \overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$. The bottleneck of the computation is computing the class and unit groups of the number fields K_h, for $h \in \mathcal{F}_{\mathbb{Q}}$, which are needed for the construction of $A(q, \mathbf{S})$.

Also, although Corollary 2.3.15 indicates that the algorithm computes $\text{Sel}^{(\mu)}(C, \mathbb{Q})$ in a finite amount of time, the size of S_{up} is prohibitively large and in general we can only hope to get information using small primes. Nevertheless we can still put the algorithm to good use as in most cases bigger primes do not have a contribution in cutting down the set we already have.

2.4 Examples

In this section we give examples of how descent on superelliptic curves can be used to tackle some interesting number theoretical problems. Example 2.4.1 is a preparatory example to demonstrate how the results from the local computations are obtained and combined to prove statements regarding the sets of rational points of the curve, or curves in question. In Example 2.4.2 we show how descent can sometimes be the appropriate technique for solving generalized Fermat equations. In Example 2.4.3 we consider a superelliptic curve, which although covers a plane cubic curve in an obvious way ($X \mapsto$

$X^2, Z \mapsto Z^2$), the set of rational points of this curve is infinite, so it is impossible to construct the set of rational points of the superelliptic curve by pulling back rational points of the cubic curve. After using the algorithm described above we exclude all but one of the covers D_α due to local insolubility and we manage to compute all the rational points of this remaining cover D_1 by other means (found in [5],[6],[7],[21]). Finally, we compute $C(\mathbb{Q})$ since $C(\mathbb{Q}) = \phi_1(D_1(\mathbb{Q}))$. The reasoning of this example, i.e. using covering techniques to transfer the problem to a different type of curves, is also used in the proof of Theorem 2.4.5, but unlike Example 2.4.3, all the curves involved can be defined over $\mathbb{Q}$. Theorem 2.4.5 also demonstrates the significance of extending descent arguments to singular superelliptic curves.

Example 2.4.1. Consider the curve defined by the equation

$$y^5 = 2x^5 + x^4 + 2x^3 + x^2 + 3x + 3.$$

This is ELS, but after applying the algorithm to this curve we obtain the results shown in Table 2.1.

p	1	2	3	5 ... 17	19 ... 37	41
$\#\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C(\mathbb{Q}_l)))$	25	25	25	2 ... 2	1 ... 1	0

Table 2.1: Descent computation for $C : y^5 = 2x^5 + x^4 + 2x^3 + x^2 + 3x + 3$.

Therefore

$$\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) \cap r_5^{-1}\left(\mu_{\mathbb{Q}_5}(C(\mathbb{Q}_5))\right) \cap r_{19}^{-1}\left(\mu_{\mathbb{Q}_{19}}(C(\mathbb{Q}_{19}))\right) \cap r_{41}^{-1}\left(\mu_{\mathbb{Q}_{41}}(C(\mathbb{Q}_{41}))\right) = \emptyset$$

which proves that $C(\mathbb{Q}) = \emptyset$. ⊠

Example 2.4.2. In [27], Halberstadt and Kraus, consider the following four generalized

Fermat equations

$$16a^7 + 87b^7 + 625c^7 = 0 \tag{2.4.1}$$

$$11a^5 + 29b^5 + 81c^5 = 0 \tag{2.4.2}$$

$$27a^5 + 16b^5 + 2209c^5 = 0 \tag{2.4.3}$$

$$32a^7 + 81b^7 + 187c^7 = 0 \tag{2.4.4}$$

These have solutions everywhere locally, but appear to have no rational points. The authors explain how the modular approach fails to show that the set of rational points is empty. We show how one can use descent to tackle all four of them.

Observe that the problem can be easily transferred to the one of finding rational points on superelliptic curves.

$$(2.4.1) \Leftrightarrow (-b, 2a, -c) \in C_1(\mathbb{Q}), \text{ where } C_1 : Y^7 = 8(87X^7 + 625Z^7)$$

$$(2.4.2) \Leftrightarrow (-a, 3c, -b) \in C_2(\mathbb{Q}), \text{ where } C_2 : Y^5 = 3(11X^5 + 29Z^5)$$

$$(2.4.3) \Leftrightarrow (-a, 2b, -c) \in C_3(\mathbb{Q}), \text{ where } C_3 : Y^5 = 2(27X^5 + 2209Z^5)$$

$$(2.4.4) \Leftrightarrow (-b, 2a, -c) \in C_4(\mathbb{Q}), \text{ where } C_4 : Y^7 = 4(81X^7 + 187Z^7)$$

Table 2.2 contains the results obtained when we perform descent on these curves.

p	1	2	3	5	7 ... 23	29
$\#\overline{Ш}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_1(\mathbb{Q}_l)))$	49	0				
$\#\overline{Ш}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_2(\mathbb{Q}_l)))$	0					
$\#\overline{Ш}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_3(\mathbb{Q}_l)))$	5	5	5	1	1 ... 1	0
$\#\overline{Ш}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_4(\mathbb{Q}_l)))$	7	0				

Table 2.2: Results for the generalized Fermat curves

Therefore $C_i(\mathbb{Q}) = \emptyset$ for $i = 1, 2, 3, 4$. $\boxtimes$

Example 2.4.3. Consider the curve C in $\mathbb{P}^2(1, 2, 1)$, defined by

$$(X, Y, Z) \in C \Leftrightarrow Y^3 = (X^2 - 3Z^2)(X^4 - 2Z^4).$$

This curve has three points at infinity $(1, 1, 0)$, $(1, \rho, 0)$ and $(1, \rho^2, 0)$, where ρ is a primitive cube root of unity. So we know that it has at least one rational point. After applying the algorithm to this curve we obtain the results shown in Table 3.5.

p	1	2	3	5	7	11	13	17 ...
$\#\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C(\mathbb{Q}_l)))$	243	243	9	3	3	3	3	1 ...

Table 2.3: Results for $C : y^3 = (x^2 - 3)(x^4 - 2)$.

The element of $\overline{\mathfrak{H}}_{\mathbb{Q}}(\mathbf{S})$ remaining is the image of the point $(1, 1, 0)$ under $\mu_{\mathbb{Q}}$ which is equal to the identity element $1_{\mathbb{Q}^* A^{*3}}$. This corresponds to a cover $\phi_1 : D_1 \to C$, where D_1 is a curve in $\mathbb{P}^5 \times C$ defined as in (2.3.3), whose set of rational points is non-empty. We fix embeddings of $K_{(x^2-3)}$ and $K_{(x^4-2)}$ in $\overline{\mathbb{Q}}$ and index the six elements of $\Theta_{\overline{\mathbb{Q}}}$ as $\vartheta_1 = \sqrt{3}, \vartheta_2 = -\sqrt{3}, \vartheta_3 = \sqrt[4]{2}, \vartheta_4 = -\sqrt[4]{2}, \vartheta_5 = i\sqrt[4]{2}$ and $\vartheta_6 = -i\sqrt[4]{2}$. D_1 is defined by the following relations

$$\begin{aligned}((u_1, \ldots, u_6), (X, Y, Z)) \in D_1 \Leftrightarrow \exists \lambda \neq 0 \text{ such that} \quad & \lambda u_j^3 = X - \vartheta_j Z \\ & \text{for } 1 \leq j \leq 6 \text{ and} \\ & \lambda^2 \prod_{j=1}^{6} u_j = Y\end{aligned}$$

This covers a curve E' of genus 1 in $\mathbb{P}^2$, defined over the number field $L := \mathbb{Q}(\vartheta_3)$, given by the equation

$$(U, V, W) \in E' \Leftrightarrow \quad V^3 = (U - \vartheta_3 W)(U^2 + \vartheta_3^2 W^2).$$

We have the following commutative diagram:

$$\begin{array}{ccc} D_1 & \xrightarrow{\phi} & C \\ {\scriptstyle\kappa}\downarrow & & \downarrow \\ E' & \xrightarrow[\tau]{} & \mathbb{P}^1 \end{array} \qquad \begin{array}{ccc} ((u_1,\ldots,u_6),(X,Y,Z)) & \longmapsto & (X,Y,Z) \\ \downarrow & & \downarrow \\ (Xu_3^2,(X-\vartheta_3 Z)u_5u_6,Zu_3^2) & \longmapsto & (X,Z) \end{array}$$

Note that κ is a well defined rational map between two non-singular curves so it is actually a morphism. We can put E' into Weierstrass form via a linear transformation, by moving the point $(\vartheta_3, 0, 1)$ to ∞. We obtain the Weierstrass model

$$E : y^2z - 8\vartheta_3^2yz^2 = x^3 - 64z^3.$$

The isomorphism of the two models is given by

$$\psi : E \to E', \qquad \psi(x,y,z) = (\vartheta_3 y, 2\vartheta_3^3 x, y - 8\vartheta_3^2 z).$$

Using the package MAGMA we find that the Mordell-Weil rank of $E(L)$ is 1. Since

$$\tau\left(\kappa\left(\phi^{-1}(C(\mathbb{Q}))\right)\right) \subseteq \mathbb{P}^1(\mathbb{Q}),$$

we are not interested in all the L-rational points of E', only $(U,V,W) \in E'(L)$ such that $(U,W) \in \mathbb{P}^1(\mathbb{Q})$. Determining these will give us $C(\mathbb{Q})$. To solve this problem we can use "Elliptic curve Chabauty" ([5],[6],[7],[21]). Fortunately this is implemented in MAGMA. Using the inbuilt MAGMA commands we find that

$$\{(U,V,W) \in E'(L) : (U,W) \in \mathbb{P}^1(\mathbb{Q})\} = \{(1,1,0),(0,-\vartheta_3,1)\}.$$

We deduce that $C(\mathbb{Q}) = \{(1,1,0)\}$. ⊠

Example 2.4.4. In [3], [26], [40] and [45] the authors consider a generalization of Lucas "Square Pyramid" problem, namely the determination of all pairs $(a,b) \in \mathbb{Z}_{>0}^2$ that satisfy

the equation

$$b^q = 1^k + 2^k + \ldots + a^k$$

for some $q \geq 2$ and $k \geq 1$. Theorem 2.4.5 below is already proved in [3] where the authors determine all the solutions for all values of q and for $1 \leq k \leq 11$. It is suggested in [2] that this could have been extended to larger values of k. Nevertheless, we present here this special case since our proof, which involves descent, includes the determination of the full set of rational points (as opposed to the subset of integral points) of a singular superelliptic curve of genus 7. We prove the case with $q = 3$ because current tools only allow the use of cubic curves for the intermediate steps[2]. We consider the case with $k = 9$ since this is a value of k where the superelliptic curve involved in the computation is both singular and non-hyperelliptic.

Theorem 2.4.5. *The only pair* $(a, b) \in \mathbb{Z}^2_{>0}$ *satisfying*

$$b^3 = \sum_{i=1}^{a} i^9$$

is $(1, 1)$.

Proof. After replacing the right hand side of the equation by the closed formula for the sum of the first a ninth powers we get the equation

$$b^3 = \frac{1}{10}a^2(a+1)^2(a^2+a-1)\left(a^4 + 2a^3 - \frac{1}{2}a^2 - \frac{3}{2}a + \frac{3}{2}\right) \tag{2.4.5}$$

After the change of variables in the proof of Proposition 1.3.9, we see that the solutions (a, b) correspond to rational points on genus 7, singular, superelliptic curve C in $\mathbb{P}^2(1, 4, 1)$ defined by

$$Y^3 = X^2(X+5Z)^2(X+10Z)^2(X^2+30XZ+100Z^2)(X^4+30X^3Z+460X^2Z^2+2400XZ^3+4000Z^4).$$

[2] Although recent developments, like the implementation of descent on Jacobian varieties of superelliptic curves in MAGMA, suggest that Chabauty's method for superelliptic curves should be available in the near future, which would open the possibility to solve cases with $q > 3$. For more details see Section 4.2.

To be precise, the map sending a solution (a, b) to a point on C is

$$(a, b) \mapsto (10, 10000b, (a-1)) \in C(\mathbb{Q}). \tag{2.4.6}$$

We have the descent map $\mu_{\mathbb{Q}} : C(\mathbb{Q}) \to A^*_{\mathbb{Q}}/\mathbb{Q}^* A^{*3}_{\mathbb{Q}}$ where the algebra $A_{\mathbb{Q}}$ is isomorphic to the product $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times K_1 \times K_2$ where $K_1 = \mathbb{Q}[x]/(x^2 + 30x + 100)$ and $K_2 = \mathbb{Q}[x]/(x^4 + 30x^3 + 460x^2 + 2400x + 4000)$. Denote the images of x in K_1 and K_2 by θ_1 and θ_2 respectively. We can compute representatives in $A^*_{\mathbb{Q}}$ for the images of the five known rational points. These are shown in Table 2.4.

i	$P_i \in C(\mathbb{Q})$	$\mu_{\mathbb{Q}}(P_i)$
1	$(1, 1, 0)$	$[(1, 1, 1, 1, 1)]$
2	$(0, 0, 1)$	$[(1, 5, 10, \theta_1, \theta_2)]$
3	$(-5, 0, 1)$	$\left[(1, 75, 1, 1, 400(5\theta_2^3 + 134\theta_2^2 + 1860\theta_2 - 5840))\right]$
4	$(-10, 0, 1)$	$\left[(2, 1, 300, 25(3\theta_1 + 10), 20(\theta_2^3 + 20\theta_2^2 - 90\theta_2 - 700))\right]$
5	$(-10, 1000, 3)$	$\left[(2, 1, 4, 25(3\theta_1 + 10), 20(13\theta_2^3 + 330\theta_2^2 + 4380\theta_2 + 9600))\right]$

Table 2.4: Representatives in $A^*_{\mathbb{Q}}$ of images of known points.

By Proposition 2.3.12, the genus G of the covers D_α is

$$G = q^{d-2}\left(\frac{d(q-1)}{2} - q\right) + 1 = 3^7\left(\frac{9 \times 2}{2} - 3\right) + 1 = 13123$$

so the set S_{up} (see Definition 2.3.13) contains the rational primes which are less than $4 \times 13123^2 = 688852516$. Performing the local computations for all of these primes would be unfeasible, but we do not need to, since after checking the primes 2, 3 and 5 we exclude every element from $\text{Ш}_{\mathbb{Q}}(\mathbf{S})$ apart from the five we already know. Thus

$$\text{Sel}^{(\mu)}(C, \mathbb{Q}) = \mu_{\mathbb{Q}}\left(\{P_1, P_2, P_3, P_4, P_5\}\right).$$

These elements correspond to five covers $\phi_i : D_i \to C$, where each D_i is a curve in $\mathbb{P}^8 \times C$, defined using a representative in $\mu_{\mathbb{Q}}(P_i)$ (see (2.3.3)).

Now for each $1 \leq i \leq 5$, we choose a combination of three factors from $\mathcal{F}_{\overline{\mathbb{Q}}}$ to form

a cover $\kappa_i : D_i \to E_i$ where E_i is a genus one curve. By choosing factors whose product is defined over $\mathbb{Q}$, we ensure that E_i and κ_i are defined over $\mathbb{Q}$. When choosing the three factors we also aim to obtain an elliptic curve E_i which has finitely many rational points. As it turns out, for all $1 \leq i \leq 5$, the subset $\{x, x+5, x+10\} \subseteq \mathcal{F}_{\overline{\mathbb{Q}}}$ satisfies the criteria we need, giving the five curves in Table 2.5.

i	$(U,V,W) \in E_i \Leftrightarrow$	$\kappa_i\left((u_h)_{h\in\mathcal{F}_{\overline{\mathbb{Q}}}}, (X,Y,Z)\right) =$
1	$V^3 = U(U+5W)(U+10W)$	$\left(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\right)$
2	$50V^3 = U(U+5W)(U+10W)$	$\left(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\right)$
3	$75V^3 = U(U+5W)(U+10W)$	$\left(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\right)$
4	$600V^3 = U(U+5W)(U+10W)$	$\left(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\right)$
5	$8V^3 = U(U+5W)(U+10W)$	$\left(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\right)$

Table 2.5: The cubic curves E_i and the maps $\kappa_i : D_i \to E_i$.

We note that there are isomorphisms $E_1 \cong E_5$ and $E_3 \cong E_4$ over $\mathbb{Q}$, but this is not relevant to the computation. We leave the coefficients of V^3 in E_4 and E_5 unchanged to remind the reader that they originate from multiplying the first three entries of the representatives of $\mu_{\mathbb{Q}}(P_i)$ shown in Table 2.4. All five cubic curves are elliptic curves with Mordell-Weil rank equal to 0 so we can determine the sets $E_i(\mathbb{Q})$.

$$E_1(\mathbb{Q}) = \left\{ \begin{array}{c} (0,0,1), (-10,-10,3), (-20,10,3), \\ (-10,0,1), \boxed{(1\ ,\ 1\ ,\ 0)}, (-5,0,1) \end{array} \right\}$$

$$E_2(\mathbb{Q}) = \left\{ \boxed{(0\ ,\ 0\ ,\ 1)}, (-10,0,1), (-5,0,1) \right\}$$

$$E_3(\mathbb{Q}) = \left\{ (0,0,1), (-10,0,1), \boxed{(\text{-}5\ ,\ 0\ ,\ 1)} \right\}$$

$$E_4(\mathbb{Q}) = \left\{ (0,0,1), \boxed{(\text{-}10\ ,\ 0\ ,\ 1)}, (-5,0,1) \right\}$$

$$E_5(\mathbb{Q}) = \left\{ \begin{array}{c} (0,0,1), (-10,0,1), (-5,0,1), \\ (-20,5,3), (2,1,0), \boxed{(\text{-}10\ ,\ \text{-}5\ ,\ 3)} \end{array} \right\}$$

We then compute the pre-images of these sets under the maps κ_i. The box indicates that

a point has one $\mathbb{Q}$-rational point in its κ_i-fiber. The rest of the points have no rational pre-image. As expected, $D_i(\mathbb{Q})$ contains exactly one element for each $1 \leq i \leq 5$. Using Corollary 2.3.9 we get

$$C(\mathbb{Q}) = \bigcup_{i=1}^{5} \phi_i \left(D_i(\mathbb{Q}) \right) = \{P_1, P_2, P_3, P_4, P_5\}.$$

These points correspond to all solutions $(a, b) \in \mathbb{Q}^2$ satisfying Equation (2.4.5). In particular, using the inverse of the map (2.4.6) we get that P_1, P_2, P_3, P_4 and P_5 correspond to $(1, 1)$, "∞", $(-1, 0)$, $(0, 0)$ and $(-2, 1)$ respectively. Therefore $(1, 1)$ is the only solution where both a and b are positive integers. □

⊠

Chapter 3

Extending "Elliptic Curve Chabauty" to higher genus curves

3.1 Preface

3.1.1 Background

As we have already shown in Section 1.3.3, the method of Chabauty and Coleman ([11],[13]) is a very well established and explicit technique used to provide reasonable and sometimes sharp upper bounds on the size of the set of rational points of a curve defined over $\mathbb{Q}$. To determine the actual set of rational points, it is usually used in combination with the Mordell-Weil sieve which was presented in Section 1.3.4. One first splits the analytic set of $\mathbb{K}_{\mathfrak{p}}$-rational points of the curve into a finite disjoint collection of neighborhoods, or residue classes. Then, Chabauty's argument, made effective using Coleman's integration on these rigid analytic spaces [14], often allows one to show that the classes containing known $\mathbb{K}$-rational points do not contain any other rational points. The Mordell-Weil sieve is then used to prove that the remaining classes (i.e the ones that appear to have no $\mathbb{K}$-rational points), indeed have none. The limitation of this approach is the fact that it only applies to curves whose Jacobians have Mordell-Weil rank less

than or equal to $g-1$, where g is the genus of the curve.

In a more recent development, Siksek ([48]) following unpublished work of Wetherell, showed that when Chabauty's method is generalized to deal with curves defined over a number field of degree $d > 1$, the limitation is usually weakened and the technique can be applied to curves whose Jacobians have Mordell-Weil rank less than or equal to $d(g-1)$. The final remark in his paper is what actually motivated the results obtained in this chapter.

Often, when one is interested in the set of rational points on a curve Υ defined over a smaller number field $\mathbb{E} \subset \mathbb{K}$, a descent argument leads to the consideration of the following problem: let C be a curve over a number field $\mathbb{K}$. Let $\psi : C \to \mathbb{P}^1$ be a morphism defined over $\mathbb{K}$. Determine the set

$$\{P \in C(\mathbb{K}) : \psi(P) \in \mathbb{P}^1(\mathbb{E})\}. \tag{3.1.1}$$

For example, Flynn and Wetherell in [21] and Bruin in ([5]), present an approach to this when C is a curve of genus 1 using a variant of Chabauty called "Elliptic Curve Chabauty". The addition of this new ingredient to the classical approach allowed Bruin to determine all solutions in coprime integers to the generalized Fermat equations

$$x^2 \pm y^4 = z^5 \qquad \text{and} \qquad x^8 + y^3 = z^2.$$

Other examples where this technique was applied to solve interesting Diophantine equations can also be found in [7], [16] and [22]. In this chapter we explain an extension of this method to curves C with genus greater than 1. The fact that we are interested not in all $\mathbb{K}$-rational points of C, but in the subset (3.1.1) allows us to weaken the Chabauty limitation on ranks even further.

Remark 3.1.1. Let J be the Jacobian of C. Our method requires knowledge of a subgroup L of $J(\mathbb{K})$ of finite index. Such a subgroup can sometimes, though not always, be

computed through a descent calculation (for genus 2 curves see [51]; for cyclic covers of the projective line see [43]). ⊠

3.1.2 Chapter structure

In Section 3.1.3 we start by setting up the notation and presenting how the two techniques described in the latter sections can be combined to determine the set of rational points of an algebraic curve.

In Section 3.2 the modified version of Chabauty is presented explicitly. There is a slight increase in complexity when dealing with points P_0 on the curve that are ramification points of the morphism ψ, as $\psi - \psi(P_0)$ can no longer be used as a uniformizing parameter in the neighborhoods of these points. This case is thus addressed separately from the case where ψ does not ramify at P_0. In the end of the section, we apply the results to three examples of curves defined over a quadratic extension of $\mathbb{Q}$. The outcome of these examples is used in Sections 3.3 and 3.4.

Then, in Section 3.3 we show how the classical Mordell-Weil sieve can also be adapted and refined, in order to work together with the version of Chabauty presented in Section 3.2.[1]

Finally, in Section 3.4 we give an example of a genus 6 hyperelliptic curve Υ defined over $\mathbb{Q}$ by the equation

$$\Upsilon : \quad y^2 = (x^3 + x^2 - 1)\Phi_{11}(x),$$

whose set of $\mathbb{Q}$-rational points cannot be computed using the classical Chabauty-Coleman approach. To apply "Elliptic Curve Chabauty", one needs to work over the degree 10 number field $\mathbb{Q}[t]/(\Phi_{11}(t))$, and current tools appear to be incapable of computing generators for the Mordell-Weil groups of the associated elliptic curves. We transfer this

[1] Even though variations of the Mordell-Weil sieve that work together with the method of "Elliptic Curve Chabauty" have been used on particular examples in the literature, to our knowledge, this is the first time an explicit description of this method appears in writing.

problem to a collection of auxiliary genus 2 curves $\{C_i\}_{i=1}^4$, defined over an appropriate quadratic number field $\mathbb{K}$. Even at this step the rank limiting inequalities given in [48] are not satisfied, but the inequalities that apply to our case, are. An implementation of our techniques in MAGMA([4]) is then used to successfully prove that

$$\Upsilon(\mathbb{Q}) = \{\infty\}.$$

3.1.3 Setup

Notation 3.1.2. Let $\mathbb{K}$ be a number field, $\mathcal{O}_{\mathbb{K}}$ its ring of integers and $\mathfrak{p}$ a prime of $\mathbb{K}$. If Ψ is any $\mathbb{K}$-algebra and $\psi \in \Psi$, we will denote by $\psi^{\mathfrak{p}}$, the image of ψ under the injection $\Psi \to \Psi \otimes_{\mathbb{K}} \mathbb{K}_{\mathfrak{p}}$, where $\mathbb{K}_{\mathfrak{p}}$ is the completion of $\mathbb{K}$ at $\mathfrak{p}$. ⊠

Definition 3.1.3. (1) Let $\mathbb{Q} \subset \mathbb{K}$ be a finite field extension. Let V be a non-singular projective algebraic variety defined over $\mathbb{K}$ and let p be a rational prime, unramified in $\mathbb{K}$, such that $V_{\mathfrak{p}}$ has good reduction for every prime $\mathfrak{p}$ of $\mathbb{K}$ such that $\mathfrak{p} \mid p$. Denote the residue field by $\mathbb{F}_{\mathfrak{p}}$. We define $\mathrm{Red}_p : V(\mathbb{K}) \to \prod_{\mathfrak{p}|p} \overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ to be the diagonal product of the usual reduction maps $\mathrm{Red}_{\mathfrak{p}} : V(\mathbb{K}) \to \overline{V}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$. When V is an abelian variety, these maps are actually homomorphisms of abelian groups.

(2) Let C be a non-singular projective algebraic curve. For $\mathcal{P} \in \prod_{\mathfrak{p}|p} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$, define

$$\mathcal{B}_p(\mathcal{P}) = \{P \in C(\mathbb{K}) : \mathrm{Red}_p(P) = \mathcal{P}\}$$

and for $P_0 \in C(\mathbb{K})$ define the p-residue class of P_0 to be

$$B_p(P_0) = \mathcal{B}_p(\mathrm{Red}_p(P_0)).$$

(3) Fix a morphism $\psi : C \to \mathbb{P}^1$ defined over $\mathbb{K}$. Note that ψ can be thought of as an

element of $\mathbb{K}(C)$. Let

$$\mathcal{H} = \{\mathcal{P} \in \prod_{\mathfrak{p}|p} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) : \overline{\psi^{\mathfrak{p}}}(\mathcal{P}_{\mathfrak{p}}) = \overline{\psi^{\mathfrak{q}}}(\mathcal{P}_{\mathfrak{q}}) \in \mathbb{P}^1(\mathbb{F}_p) \quad \forall \mathfrak{p}, \mathfrak{q} \mid p\}$$

and

$$H = \psi^{-1}(\mathbb{P}^1(\mathbb{Q})) \cap C(\mathbb{K}).$$

⊠

Consider the following commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{\quad\psi\quad} & \mathbb{P}^1(\mathbb{Q}) \\ \Big\downarrow{\scriptstyle \mathrm{Red}_p} & & \Big\downarrow{\scriptstyle \mathrm{Red}_p} \\ \prod_{\mathfrak{p}|p} \overline{C}(\mathbb{F}_{\mathfrak{p}}) & \xrightarrow{\prod_{\mathfrak{p}|p} \overline{\psi^{\mathfrak{p}}}} & \prod_{\mathfrak{p}|p} \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}}) \end{array}$$

Suppose we have a subset $H^{\mathrm{search}} \subseteq H$. In practice H^{search} will be a subset of H found through a computer search. The aim of this chapter is to provide explicit techniques that often allow one to show that

(a) for all $P_0 \in H^{\mathrm{search}}$ we have that $B_p(P_0) \cap H = \{P_0\}$ (by using a modification of "Elliptic Curve Chabauty") and

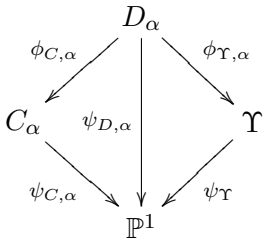
(b) for all $\mathcal{P} \in \mathcal{H} \setminus \mathrm{Red}_p(H^{\mathrm{search}})$ we have that $\mathcal{B}_p(\mathcal{P}) \cap H = \emptyset$ (by using a modification of the Mordell-Weil sieve).

(a) and (b) put together imply that $H^{\mathrm{search}} = H$.

When dealing with the problem of determination of the set $\Upsilon(\mathbb{Q})$ for an algebraic curve Υ defined over $\mathbb{Q}$, we can sometimes perform a partial[2] descent computation to

[2]The word "partial" to describe descent using only partial information arising from factorization in a smaller than usual number field was first used in [49], but the technique was also explored earlier, for example in [7].

obtain a finite collection, which we will label using a finite set $\mathcal{S}$, of commutative diagrams



(3.1.2)

for each $\alpha \in \mathcal{S}$, where D_α, $\phi_{\Upsilon,\alpha}$, ψ_Υ and $\psi_{D,\alpha}$ are defined over $\mathbb{Q}$ and C_α, $\phi_{C,\alpha}$, $\psi_{C,\alpha}$ are defined over $\mathbb{K}$. As with the usual (full) descent we have

$$\Upsilon(\mathbb{Q}) = \bigcup_{\alpha \in \mathcal{S}} \phi_{\Upsilon,\alpha}(D_\alpha(\mathbb{Q})).$$

We note that

$$D_\alpha(\mathbb{Q}) \subseteq D_\alpha(\mathbb{K}) \subseteq \phi_{C,\alpha}^{-1}(C_\alpha(\mathbb{K}))$$

and

$$D_\alpha(\mathbb{Q}) \subseteq \psi_{D,\alpha}^{-1}(\mathbb{P}^1(\mathbb{Q})) \Rightarrow D_\alpha(\mathbb{Q}) \subseteq \phi_{C,\alpha}^{-1}(\psi_{C,\alpha}^{-1}(\mathbb{P}^1(\mathbb{Q}))),$$

so

$$D_\alpha(\mathbb{Q}) \subseteq \phi_{C,\alpha}^{-1}(\psi_{C,\alpha}^{-1}(\mathbb{P}^1(\mathbb{Q})) \cap C_\alpha(\mathbb{K})).$$

We can then employ our Chabauty-Coleman/Mordell-Weil sieve argument to compute $D_\alpha(\mathbb{Q})$ for each $\alpha \in \mathcal{S}$ and thus determine $\Upsilon(\mathbb{Q})$.

Example 3.1.4. Let Υ be the genus 6 hyperelliptic curve which has an affine patch[3] defined by the equation

$$\begin{aligned} y^2 &= (x^3 + x^2 - 1)\Phi_{11}(x) \\ &= x^{13} + 2x^{12} + 2x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 - x - 1. \end{aligned}$$

[3]Even though the curves found in this example are projective we only use the affine equations to define the curves and the maps involved.

We start by noticing that over $\mathbb{K} = \mathbb{Q}[x]/(x^2 - x + 3) = \mathbb{Q}(\theta)$

$$(x^3 + x^2 - 1)\Phi_{11}(x) = (x^3 + x^2 - 1)f(x)g(x),$$

where

$$\begin{aligned} f(x) =& x^5 + \theta x^4 - x^3 + x^2 + (\theta - 1)x - 1 \\ g(x) =& x^5 + (-\theta + 1)x^4 - x^3 + x^2 - \theta x - 1. \end{aligned}$$

This decomposition over $\mathbb{K}$ suggests that a partial descent argument can be used. So we define a map

$$\mu : \Upsilon(\mathbb{Q}) \to \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right) \times \left(\mathbb{K}^*/\mathbb{K}^{*2}\right),$$

$$\mu(P) = \begin{cases} \left((x^3 + x^2 - 1)\mathbb{Q}^{*2}, f(x)\mathbb{K}^{*2}\right) & \text{, if } P = (x, y) \\ \left((1)\mathbb{Q}^{*2}, (1)\mathbb{K}^{*2}\right) & \text{, if } P = \infty \end{cases}.$$

The image of this map is contained in

$$\text{Kernel}\left(\overline{\mathcal{N}}\right) \cap \left(\mathbb{Q}(2, S_1) \times \mathbb{K}(2, S_2)\right),$$

where $S_1 = \text{Supp}(\text{Resultant}(x^3+x^2-1, f(x)g(x))) = \{23\}$, $S_2 = \text{Supp}(\text{Resultant}(f(x), (x^3+x^2-1)g(x))) = \{\mathfrak{p}\}$, with $\mathfrak{p}$ one of the primes of $\mathcal{O}_{\mathbb{K}}$ above 23, and

$$\overline{\mathcal{N}} : \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right) \times \left(\mathbb{K}^*/\mathbb{K}^{*2}\right) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$

the reduction of the product of norm maps

$$\mathcal{N} : \mathbb{Q} \times \mathbb{K} \to \mathbb{Q},$$

$$\mathcal{N}(h_1, h_2) = h_1 \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(h_2).$$

Also for each element $\alpha = (\alpha_1, \alpha_2)$ in the image of μ, we can associate a cover $\phi_{\Upsilon,\alpha} : D_\alpha \to \Upsilon$ defined by

$$D_{(\alpha_1,\alpha_2)} : \begin{cases} y_1^2 = \alpha_1(x^3 + x^2 - 1) \\ y_2^2 = \alpha_2 f(x) \\ y_3^2 = \sigma(\alpha_2) g(x) \end{cases} \quad \text{and}$$

$$\phi_{\Upsilon,\alpha}(x, y_1, y_2, y_3) = (x, \nu y_1 y_2 y_3),$$

where σ is the non-trivial automorphism of $\mathbb{K}$ and ν is a rational number satisfying $\nu^2 \alpha_1 \mathcal{N}_{K/\mathbb{Q}}(\alpha_2) = 1$. The D_α's are products of curves, fibered over $\mathbb{P}^1$. Note that the D_α's are actually defined over $\mathbb{Q}$[4]. These are in turn covered by the D_α's of full descent found in Section 2.3.2, but we use the same notation since we will not need both sets of covers in this example. More details on these "towers of covers" and the relation with the Galois group associated with the defining equation of Υ can be found in [7]. If we set $\mathcal{S} = \text{Image}(\mu)$ we get

$$\Upsilon(\mathbb{Q}) = \bigcup_{\alpha \in \mathcal{S}} \phi_{\Upsilon,\alpha}(D_\alpha(\mathbb{Q})).$$

A computation gives that

$$\text{Kernel}(\overline{\mathcal{N}}) \cap (\mathbb{Q}(2, S_1) \times \mathbb{K}(2, S_2)) = \{(1,1), (1,-1), (23, 5-\theta), (23, \theta - 5)\},$$

[4]This is because a point on the projective model of D_α is of the form $(X, Y_1, Y_2, Y_3, Z) \in \mathbb{P}^4(2,3,5,5,1)$, with $\mathcal{G}_\mathbb{Q}$ acting on Y_2 and Y_3 the same way it acts on the roots of the defining polynomial of $\mathbb{K}$

so we only need to be concerned about the covers

$$D_1 = D_{(1,1)}: \quad \begin{cases} y_1^2 = x^3 + x^2 - 1 \\ y_2^2 = f(x) \\ y_3^2 = g(x) \end{cases}$$

$$D_2 = D_{(1,-1)}: \quad \begin{cases} y_1^2 = x^3 + x^2 - 1 \\ y_2^2 = -f(x) \\ y_3^2 = -g(x) \end{cases}$$

$$D_3 = D_{(23,5-\theta)}: \quad \begin{cases} y_1^2 = 23(x^3 + x^2 - 1) \\ y_2^2 = (5-\theta)f(x) \\ y_3^2 = (\theta+4)g(x) \end{cases}$$

$$D_4 = D_{(23,\theta-5)}: \quad \begin{cases} y_1^2 = 23(x^3 + x^2 - 1) \\ y_2^2 = -(5-\theta)f(x) \\ y_3^2 = -(\theta+4)g(x) \end{cases}$$

and the corresponding covering maps

$$\phi_{\Upsilon,i} : D_i \to \Upsilon, \qquad \phi_{\Upsilon,i}(x, y_1, y_2, y_3) = \begin{cases} (x, y_1y_2y_3) & \text{for } i = 1, 2 \\ \left(x, \frac{1}{23}y_1y_2y_3\right) & \text{for } i = 3, 4. \end{cases}$$

These cover, over $\mathbb{K}$, the genus 2 curves

$$C_1: \quad y^2 = f(x) \tag{3.1.3}$$

$$C_2: \quad y^2 = -f(x) \tag{3.1.4}$$

$$C_3: \quad y^2 = (5-\theta)f(x) \tag{3.1.5}$$

$$C_4: \quad y^2 = -(5-\theta)f(x) \tag{3.1.6}$$

respectively, via the maps

$$\phi_{C,i} : D_i \to C_i, \quad \phi_{C,i}(x, y_1, y_2, y_3) = (x, y_2).$$

All $\mathbb{Q}$-rational points of the D_i's have $\mathbb{Q}$-rational x-coordinate so we can use the maps

$$\begin{aligned} \psi_\Upsilon &: \Upsilon \to \mathbb{P}^1 & \psi_\Upsilon(x, y) &= (x, 1) \\ \psi_{D,i} &: D_i \to \mathbb{P}^1 & \psi_{D,i}(x, y_1, y_2, y_3) &= (x, 1) \\ \psi_{C,i} &: C_i \to \mathbb{P}^1 & \psi_{C,i}(x, y) &= (x, 1) \end{aligned}$$

to form the data in (3.1.2). Later on, in Lemma 3.3.3, we will compute the sets

$$\psi_{C,i}^{-1}(\mathbb{P}^1(\mathbb{Q})) \cap C_i(\mathbb{K})$$

for $1 \leq i \leq 4$, which are required for the determination of $\Upsilon(\mathbb{Q})$ in Theorem 3.4.1. ⊠

3.2 Chabauty

Let $\mathbb{K}$, C, J and $\psi : C \to \mathbb{P}^1$ have their usual meaning. We will be using $P_0 \in H^{\text{search}}$ as a basepoint for the embedding $\iota : C \to J$, but in practice the process described in this section has to be repeated for each $P_0 \in H^{\text{search}}$. When this is completed or if H^{search} is empty, then one should use some $D \in J(\mathbb{K})$ with $\deg(D) = 1$ to define the embedding ι and perform the Mordell-Weil sieve described in Section 3.3. If no such D can be found, then hopefully $C(\mathbb{K})$ can be shown to be empty using descent computations.

An essential ingredient in what will follow, is the use of uniformizing parameters to linearize the neighborhoods of the analytic spaces $C_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$ and $J_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$, for some prime $\mathfrak{p}$ of $\mathbb{K}$, thus reducing the problem of finding points on varieties to simple linear algebra. We will require our uniformizers to be "well-behaved" under reduction.

Definition 3.2.1. Suppose $P_0 \in C_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$. We call a function $\tau^\mathfrak{p} \in \mathbb{K}_\mathfrak{p}(C_\mathfrak{p})$ a **well-**

behaved uniformizer of $C_{\mathfrak{p}}$ **at** P_0 when

(i) $\tau^{\mathfrak{p}}$ is a uniformizer of $C_{\mathfrak{p}}$ at P_0 and

(ii) $\overline{\tau^{\mathfrak{p}}}$ is a uniformizer of $\overline{C}_{\mathfrak{p}}$ at $\mathrm{red}_{\mathfrak{p}}(P_0)$.

⊠

Lemma 3.2.2. *Let $\tau^{\mathfrak{p}}$ be a well-behaved uniformizer of $C_{\mathfrak{p}}$ at P_0 and π be a uniformizing element for $\mathbb{K}_{\mathfrak{p}}$. Then the map defined by $B_{\mathfrak{p}}(P_0) \to \pi\mathcal{O}_{\mathfrak{p}}, \quad P \mapsto \tau^{\mathfrak{p}}(P)$ is a bijection. In particular, if $P \in B_{\mathfrak{p}}(P_0)$ and $P \neq P_0$ then $\tau^{\mathfrak{p}}(P) \neq 0$.*

Proof. This is a standard result, see for example [35, Section 1] or [56, Sections 1.7 and 1.8]. □

The idea behind both "Elliptic Curve Chabauty" and our method, is to exploit the extra dimensions over $\mathbb{Q}$, when working in a number field $\mathbb{K}$, so that the number of *equations* gets multiplied by $d = [\mathbb{K} : \mathbb{Q}]$, while the number of *unknowns* remains the same, since they are defined over $\mathbb{Q}$. For the sake of argument suppose $[\mathbb{K} : \mathbb{Q}] = d$ and that we have a rational prime p such that $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}$. To see what is going on geometrically, let $\mathcal{R}_{\mathfrak{p}/p}$ denote the Weil restriction of scalars functor from varieties over $\mathbb{K}_{\mathfrak{p}}$ to varieties over $\mathbb{Q}_p$. Consider the following diagram:

$$\begin{array}{ccc} \mathcal{R}_{\mathfrak{p}/p}(C) & \xhookrightarrow{\mathcal{R}_{\mathfrak{p}/p}(\iota)} & \mathcal{R}_{\mathfrak{p}/p}(J) \\ & & \downarrow{\scriptstyle \mathcal{R}_{\mathfrak{p}/p}(\psi^{\mathfrak{p}})} \\ \mathbb{P}^1(\mathbb{Q}_p) & \xhookrightarrow{\qquad} & \mathcal{R}_{\mathfrak{p}/p}(\mathbb{P}^1) \end{array}$$

Instead of taking the intersection in the gd-dimensional $\mathcal{R}_{\mathfrak{p}/p}(J_{\mathfrak{p}})(\mathbb{Q}_p)$ of the d- dimensional $\mathcal{R}_{\mathfrak{p}/p}(\iota)\left(\mathcal{R}_{\mathfrak{p}/p}(C_{\mathfrak{p}})(\mathbb{Q}_p)\right)$ with the $\leq r$-dimensional $J(\mathbb{K})^{cl}$, we only need the intersection of the latter with the 1-dimensional

$$\mathcal{R}_{\mathfrak{p}/p}(\iota)\left(\mathcal{R}_{\mathfrak{p}/p}(\psi^{\mathfrak{p}})^{-1}(\mathbb{P}^1(\mathbb{Q}_p))\right),$$

so when $gd - 1 \geq r$, the dimensions suggest that this intersection is finite.

When ψ is ramified at P_0, then one of our unknowns, namely our uniformizer evaluated at a point, $\tau(P)$, is no longer guaranteed to be $\mathbb{Q}_p$-rational, so we have to put in extra effort to find new $\mathbb{Q}_p$-rational relations and unknowns. At the moment, we know how to do this using rational primes p that do not ramify in quadratic number fields, or split completely in general number fields.

3.2.1 Unramified case

Let C be a non-singular, projective, genus g, algebraic curve defined over a number field $\mathbb{K}$ and $\psi : C \to \mathbb{P}^1$ a morphism to $\mathbb{P}^1$ which is also defined over $\mathbb{K}$. Suppose $P_0 \in H = \psi^{-1}\left(\mathbb{P}^1(\mathbb{Q})\right) \cap C(\mathbb{K})$. Suppose further that ψ is unramified at P_0. If $\psi(P_0) = \infty$ replace ψ by $1/\psi$. Now fix a rational prime p such that:

(p1) p does not ramify in $\mathbb{K}$, i.e. $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1 \dots \mathfrak{p}_m$ with the $\mathfrak{p}_i$ distinct prime ideals.

(p2) $C_{\mathfrak{p}_i} = C \times_{\mathbb{K}} \mathbb{K}_{\mathfrak{p}_i}$ has good reduction for $1 \leq i \leq m$.

(p3) The reduced point $\mathrm{red}_{\mathfrak{p}_i}(P_0)$ is not a ramification point of the reduced map $\overline{\psi^{\mathfrak{p}_i}}$ for $1 \leq i \leq m$.

We aim to find a criterion that will guarantee that $B_p(P_0) \cap H = \{P_0\}$.

Fix $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$. Let $\mathcal{C}$ be a proper regular minimal model for C over $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}$. Now $\tau := \psi - \psi(P_0) \in \mathbb{K}(C)$ is a uniformizer for C at P_0. By **(p1)**, **(p2)** and **(p3)**, $\tau^{\mathfrak{p}}$ is a well-behaved uniformizer for the generic fiber $\mathcal{C}_{\mathrm{gen}} = C_{\mathfrak{p}}$ at P_0 and $\overline{\tau^{\mathfrak{p}}}$ is a uniformizer for the special fiber $\mathcal{C}_{\mathrm{sp}} = \overline{C}_{\mathfrak{p}}$ at $\mathrm{red}_{\mathfrak{p}}(P_0)$. Let $P \in B_p(P_0) \cap H$. In order to think in terms of matrices we will fix a basis $\omega_1^{\mathfrak{p}}, \dots, \omega_g^{\mathfrak{p}}$ for the $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}$-module $H^0(\mathcal{C}, \Omega^1)$ of holomorphic 1-forms on $\mathcal{C}$ and also a finite index subgroup, $L = \langle D_1, \dots, D_r \rangle$, of the Mordell-Weil group $J(\mathbb{K})$, such that $[J(\mathbb{K}) : L] = N$. Then

$$N \cdot \iota(P) = N[P - P_0] = n_1 D_1 + \ldots + n_r D_r \tag{3.2.1}$$

in $J(\mathbb{K})$, for some $n_1, \ldots, n_r \in \mathbb{Z}$.

Note that

$$t^{\mathfrak{p}} := \tau^{\mathfrak{p}}(P) = \psi^{\mathfrak{p}}(P) - \psi^{\mathfrak{p}}(P_0) = (\psi(P) - \psi(P_0))^{\mathfrak{p}} = \psi(P) - \psi(P_0) \in \mathbb{Q}$$

for every $\mathfrak{p} \mid p$, so

$$t^{\mathfrak{p}_1} = \ldots = t^{\mathfrak{p}_m} =: t,$$

and since $\mathrm{ord}_{\mathfrak{p}_c}(t^{\mathfrak{p}_c}) \geq 1$ for $1 \leq c \leq m$ we have that $\mathrm{ord}_p(t) \geq 1$. In other words, $t \in p\mathbb{Z}_p$.

Let $\mathfrak{p} \mid p$ and $\omega \in H^0(\mathcal{C}, \Omega^1)$ be a holomorphic 1-form. We will define the matrix $A_{\mathfrak{p},\omega} \in M_{d_{\mathfrak{p}},r}(\mathbb{Q}_p)$ and the column vector $\mathbf{a}_{\mathfrak{p},\omega} \in \mathbb{Z}_p^{d_{\mathfrak{p}}}$, where $d_{\mathfrak{p}} = [\mathbb{K}_{\mathfrak{p}} : \mathbb{Q}_p]$, as follows: Using (3.2.1) and Lemma 1.3.30 together we get the following equality in $\mathbb{K}_{\mathfrak{p}}$

$$\alpha_1 n_1 + \ldots + \alpha_r n_r = \alpha t + \beta t^2, \tag{3.2.2}$$

where $\alpha_q = \int_0^{D_q} \omega$ for $1 \leq q \leq r$. Fix an integral basis $\theta_1, \ldots, \theta_{d_{\mathfrak{p}}}$ for $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$ over $\mathbb{Z}_p$. We can write $\alpha_q = a_{1,q}\theta_1 + \ldots + a_{d_{\mathfrak{p}},q}\theta_{d_{\mathfrak{p}}}$, $\alpha = a_1\theta_1 + \ldots + a_{d_{\mathfrak{p}}}\theta_{d_{\mathfrak{p}}}$ and $\beta = b_1\theta_1 + \ldots + b_{d_{\mathfrak{p}}}\theta_{d_{\mathfrak{p}}}$ and equate coefficients to get the following system of equations in $\mathbb{Q}_p$

$$\begin{aligned} a_{1,1}(n_1/N) + \ldots + a_{1,r}(n_r/N) &= a_1 t + b_1 t^2 \\ \vdots &= \vdots \\ a_{d_{\mathfrak{p}},1}(n_1/N) + \ldots + a_{d_{\mathfrak{p}},r}(n_r/N) &= a_{d_{\mathfrak{p}}} t + b_{d_{\mathfrak{p}}} t^2. \end{aligned}$$

Define $A_{\mathfrak{p},\omega} = (a_{c,q})_{1 \leq c \leq d_{\mathfrak{p}}, 1 \leq q \leq r}$ and $\mathbf{a}_{\mathfrak{p},\omega}$ to be the column vector $(a_1, \ldots, a_{d_{\mathfrak{p}}}) \in \mathbb{Z}_p^{d_{\mathfrak{p}}}$. Now define the matrix $A_{\mathfrak{p}} \in M_{gd_{\mathfrak{p}},r}(\mathbb{Q}_p)$ and the column vector $\mathbf{a}_{\mathfrak{p}} \in \mathbb{Z}_p^{gd_p}$ as

$$A_{\mathfrak{p}} = \begin{pmatrix} A_{\mathfrak{p},\omega_1^{\mathfrak{p}}} \\ \vdots \\ A_{\mathfrak{p},\omega_g^{\mathfrak{p}}} \end{pmatrix} \quad \text{and} \quad \mathbf{a}_{\mathfrak{p}} = \begin{pmatrix} \mathbf{a}_{\mathfrak{p},\omega_1^{\mathfrak{p}}} \\ \vdots \\ \mathbf{a}_{\mathfrak{p},\omega_g^{\mathfrak{p}}} \end{pmatrix}.$$

Finally define the matrix $A \in M_{dg,r}(\mathbb{Q}_p)$ and the column vector $\mathbf{a} \in \mathbb{Z}_p^{gd}$ as

$$A = \begin{pmatrix} A_{\mathfrak{p}_1} \\ \vdots \\ A_{\mathfrak{p}_m} \end{pmatrix} \quad \text{and} \quad \mathbf{a} = \begin{pmatrix} \mathbf{a}_{\mathfrak{p}_1} \\ \vdots \\ \mathbf{a}_{\mathfrak{p}_m} \end{pmatrix}.$$

We now have

$$A\mathbf{n} = t\mathbf{a} + t^2\mathbf{b},$$

where $\mathbf{n} = (n_1/N, \ldots, n_r/N) \in \mathbb{Q}^r$ and $\mathbf{b} \in \mathbb{Z}_p^{gd}$. Let h be the smallest integer such that $p^h A$ has entries in $\mathbb{Z}_p$ and U be a $(gd - r) \times (gd)$ matrix with entries in $\mathbb{Z}_p$ such that

$$\overline{U \cdot (p^h A)} \equiv \mathbf{0}$$

modulo p. Denote by $\mathcal{M}_p(P_0)$ the set containing only the column vector $U \cdot \mathbf{a}$ in $\mathbb{Z}_p^{gd-r}$. The reason for defining the set $\mathcal{M}_p(P_0)$ that only contains a single element will become apparent when we discuss how we deal with the case of ψ being ramified at P_0 in Section 3.2.2.

Theorem 3.2.3. *If $\overline{p^h A}$ has full rank and the unique $E \in \mathcal{M}_p(P_0)$ satisfies $\overline{E} \not\equiv \mathbf{0}$ modulo p, then $B_p(P_0) \cap H = \{P_0\}$.*

Proof. Let $P \in B_p(P_0)$ with $P \neq P_0$ and $\psi(P) \in \mathbb{P}^1(\mathbb{Q})$. Using the fact that $\psi - \psi(P_0)$ is a local isomorphism we see that

$$s = \mathrm{ord}_p(t)$$

is finite. We have a matrix U such that $\overline{U \cdot (p^h A)} = \mathbf{0}$ modulo p, but since $\overline{p^h A}$ has full rank, we can use Hensel's lemma to lift U to a matrix $\hat{U}$ such that $\overline{U} \equiv \overline{\hat{U}}$ and $\hat{U} \cdot A = \mathbf{0}$

(see Lemma 1.3.32). We have that

$$\mathbf{0} = \hat{U} \cdot A \cdot \mathbf{n} = t\hat{U} \cdot \mathbf{a} + t^2 \hat{U} \cdot \mathbf{b}.$$

Now divide by p^s and reduce modulo p to get

$$\mathbf{0} \equiv v\overline{\hat{U} \cdot \mathbf{a}} \equiv v\overline{U \cdot \mathbf{a}} \equiv v\overline{E} \qquad \bmod p,$$

but this is a contradiction since both $v = \overline{(t/p^s)}$ and $\overline{E}$ are non-zero. □

3.2.2 Ramified case

Suppose we have $P_0 \in H^{\text{search}}$ such that ψ ramifies at P_0. Write $e_\psi(P_0) = e$ for the ramification index of ψ at P_0. Then $e \geq 2$. Define the modified properties:

(p1)$^{\text{split}}$ $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1 \dots \mathfrak{p}_d$, in other words p splits completely into distinct primes in $\mathcal{O}_{\mathbb{K}}$, and $\gcd(p, e) = 1$.

(p1)$^{\text{inert}}$ $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}$, in other words p is inert in $\mathcal{O}_{\mathbb{K}}$.

(p3)$^{\text{ram}}$ $e_{\overline{\psi^{\mathfrak{p}}}}(\text{red}_{\mathfrak{p}}(P_0)) = e$ for every prime $\mathfrak{p} \mid p$

If $[\mathbb{K} : \mathbb{Q}] = 2$ then choose an odd rational prime p that satisfies either **(p1)$^{\text{split}}$,(p2)** and **(p3)$^{\text{ram}}$** or **(p1)$^{\text{inert}}$,(p2)** and **(p3)$^{\text{ram}}$**, otherwise choose p such that it satisfies **(p1)$^{\text{split}}$,(p2)** and **(p3)$^{\text{ram}}$**.

Proposition 3.2.4. *Let $\mathfrak{p}$ be a prime of $\mathbb{K}$. Let $P_0 \in C_{\mathfrak{p}}(\mathbb{K}_{\mathfrak{p}})$. Any function $\tau \in \mathbb{K}_{\mathfrak{p}}[C_{\mathfrak{p}}]_{P_0}$ which vanishes at P_0, and maps modulo $\mathfrak{p}$ to a uniformizer $\overline{\tau}$ at $\text{red}_{\mathfrak{p}}(P_0)$ for $\overline{C}_{\mathfrak{p}}$, is a uniformizer at P_0 for $C_{\mathfrak{p}}$. If $\zeta \in \mathbb{K}_{\mathfrak{p}}[C_{\mathfrak{p}}]_{P_0}$ vanishes at P_0, then there exists $\eta \in \mathbb{K}_{\mathfrak{p}}[C_{\mathfrak{p}}]_{P_0}$ such that $\zeta = \tau\eta$. The local power-series*

$$\zeta(\tau) = \sum_{i=0}^{\infty} \rho_i \tau^i$$

satisfies $\rho_i \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$. *Let* $P \in C_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$ *with* $\mathrm{red}_\mathfrak{p}(P) = \mathrm{red}_\mathfrak{p}(P_0)$. *Then*

$$\zeta(P) = \sum_{i=0}^{\infty} \rho_i \tau(P)^i.$$

Proof. This is Proposition 8 in [17], with the notation adapted to our case. □

Lemma 3.2.5. *Suppose* $\mathfrak{p}$ *is a prime (of* $\mathbb{K}$*) of good reduction for* C. *Let* τ *be a well-behaved uniformizer for* $C_\mathfrak{p}$ *at a point* $P_0 \in C_\mathfrak{p}(\mathbb{K}_\mathfrak{p})$ *and* $\psi^\mathfrak{p} \in \mathbb{K}_\mathfrak{p}(C_\mathfrak{p})$ *be a rational function such that* $e_{\overline{\psi^\mathfrak{p}}}(\mathrm{red}_\mathfrak{p}(P_0)) = e_{\psi^\mathfrak{p}}(P_0) = e$. *Let*

$$\upsilon\tau^e + \sum_{i=1}^{\infty} \rho_i \tau^{e+i}$$

be the powerseries expansion around P_0 *of* $\psi^\mathfrak{p} - \psi^\mathfrak{p}(P_0)$ *with respect to* τ. *Then* $\upsilon \in \mathcal{O}^*_{\mathbb{K}_\mathfrak{p}}$ *and* $\rho_i \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ *for every* i.

Proof. We can use Proposition 3.2.4 to show that, under our assumptions, all the coefficients in the expansion are in $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}$. The fact that the first $e-1$ coefficients are zero and that $\upsilon \in \mathcal{O}^*_{\mathbb{K}_\mathfrak{p}}$ is obvious due to the ramification index of $\psi^\mathfrak{p}$ at P_0. □

p splits

Let us first consider the case where $\mathbb{K}$ is a number field of degree $d > 1$ over $\mathbb{Q}$ with ring of integers $\mathcal{O}_\mathbb{K}$ and that p is an odd rational prime that splits completely into distinct primes over $\mathbb{K}$. Equivalently $p\mathcal{O}_\mathbb{K} = \mathfrak{p}_1 \dots \mathfrak{p}_d$ with each $\mathfrak{p}_c$, $1 \leq c \leq d$, a prime of $\mathcal{O}_\mathbb{K}$ of norm equal to p. To simplify the notation let $\mathbb{K}_c$ denote the completion of $\mathbb{K}$ with respect to $\mathfrak{p}_c$ and $\mathcal{O}_c$ be the ring of integers of $\mathbb{K}_c$. Also let $\mathcal{C}_c$ be a minimal, regular and proper model for $C_c = C \times_\mathbb{K} \mathbb{K}_c$ over $\mathcal{O}_c$.

Lemma 3.2.6. *Suppose that* $P_0 \in H$ *has* $e_\psi(P_0) = e \geq 2$ *and let* p *be a prime satisfying* ***(p1)^{split},(p2)*** *and* ***(p3)^{ram}***. *Let* τ_c *be a well-behaved uniformizer of* C_c *at* P_0 *and denote*

by

$$\upsilon_c T_c^e + \sum_{i=1}^{\infty} \rho_{c,i} T_c^{e+i} \in \mathbb{K}_c[[T_c]] = \mathbb{Q}_p[[T_c]]$$

the formal powerseries expansion of $\psi^{\mathfrak{p}_c} - \psi(P_0)$ *in terms of* τ_c. *Suppose there exists* $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. *Then for every* $c \in \{2, \ldots, d\}$, $\upsilon_1 T_1^e - \upsilon_c T_c^e \in \mathbb{Z}_p[T_1, T_c]$ *has a linear factor* $T_1 - \hat{\gamma}_c T_c$ *satisfying*

$$t_1 - \hat{\gamma}_c t_c \equiv 0 \mod p^{2s},$$

where $t_c := \tau_c(P)$ *for* $1 \leq c \leq d$ *and* $s = \mathrm{ord}_p(t_1) = \mathrm{ord}_p(t_c) \geq 1$.

Proof. By substituting P in the powerseries expansion of $\psi^{\mathfrak{p}_c} - \psi(P_0)$ we get the d equations

$$\psi(P)^{\mathfrak{p}_c} - \psi(P_0) = \upsilon_c t_c^e + \rho_c t_c^{e+1}.$$

Note that $\upsilon_c \in \mathbb{Z}_p^*$ and $\rho_c \in \mathbb{Z}_p$, by Lemma 3.2.5, since p satisfies $\mathbf{(p3)^{ram}}$. Since $\psi(P) \in \mathbb{Q}$ we have that

$$\psi(P)^{\mathfrak{p}_1} = \ldots = \psi(P)^{\mathfrak{p}_d} = \psi(P) \in \mathbb{Q}.$$

In particular we have that

$$\mathrm{ord}_p(t_1) = \ldots = \mathrm{ord}_p(t_d),$$

since $\upsilon_c \in \mathbb{Z}_p^*$ for every $c \in \{1, \ldots, d\}$. Let us denote this positive integer by s. We have the following $d-1$ congruences

$$\upsilon_1 t_1^e - \upsilon_c t_c^e \equiv 0 \mod p^{s(e+1)},$$

for $c \in \{2, \ldots, d\}$. By letting $\gamma_c = \frac{t_1}{t_c}$ we have that γ_c is a solution to

$$v_1 X^e - v_c \equiv 0 \mod p^s.$$

Since the derivative of this polynomial is equal to ev_1X^{e-1} and e, v_1 and γ_c are units modulo p we can use Hensel's lemma to lift γ_c to a solution $\hat{\gamma}_c \in \mathbb{Z}_p^*$. We then have that

$$(X - \hat{\gamma}_c) \mid (v_1 X^e - v_c) \quad \text{and} \quad (T_1 - \hat{\gamma}_c T_c) \mid (v_1 T_1^e - v_c T_c^e).$$

Furthermore we have that

$$\gamma_c \equiv \hat{\gamma}_c \mod p^s,$$

which implies that

$$t_1 - \hat{\gamma}_c t_c \equiv 0 \mod p^{2s}.$$

□

Let $P_0, e, p, t_1, \ldots, t_d, v_1, \ldots, v_d$ be as in the statement of Lemma 3.2.6 above. Suppose that $(X - \hat{\gamma}_c^{(1)}), \ldots, (X - \hat{\gamma}_c^{(l_c)})$ are all the linear factors of $v_1 X^e - v_c$ for $c \in \{2, \ldots, d\}$. Define the matrices $E_{(i_2,\ldots,i_d)} \in M_{d-1,d}(\mathbb{Z}_p)$ by

$$E_{(i_2,\ldots,i_d)} = \begin{pmatrix} 1 & -\hat{\gamma}_2^{(i_2)} & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \ldots & -\hat{\gamma}_d^{(i_d)} \end{pmatrix}$$

for $i_c \in \{1, \ldots, l_c\}$.

Let $\{\omega_f^c\}_{1 \le f \le g}$ be a basis of $H^0(\mathcal{C}_c, \Omega^1)$ for $1 \le c \le d$ and let $L = \langle D_1, \ldots, D_r \rangle$ be a subgroup of $J(\mathbb{K})$ of index $N \in \mathbb{Z}_{>0}$. Now fix a $c \in \{1, \ldots, d\}$. Define A_c to be the $g \times r$ matrix with entries in $\mathbb{Q}_p$ defined by $A_c = (a_{f,q})_{1 \le f \le g, 1 \le q \le r}$ where

$$a_{f,q} = \int_0^{D_q} \omega_f^c$$

and by $\mathbf{a}_c$ the $g \times d$ matrix with zero entries everywhere apart from the c-th column which will consist of the vector $(a_1, \ldots, a_g)$ where a_f is the coefficient of the linear term in the (formal) powerseries expansion of

$$\int_0^{[P-P_0]} \omega_f^c$$

in terms of τ_c (the well-behaved uniformizer of C_c at P_0). Now let A be the $dg \times r$ matrix

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_d \end{pmatrix}$$

with entries in $\mathbb{Q}_p$ and $\mathbf{a}$ be the $gd \times d$ matrix

$$\mathbf{a} = \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_d \end{pmatrix}$$

with entries in $\mathbb{Z}_p$. Let h be the smallest non-negative integer such that $p^h A$ has entries in $\mathbb{Z}_p$ and $U \in M_{dg-r,dg}(\mathbb{Z}_p)$ be a matrix such that

$$\overline{U \cdot (p^h A)} \equiv \mathbf{0} \qquad \mod p.$$

We denote by $E_0 \in M_{dg-r,d}(\mathbb{Z}_p)$ the matrix $U \cdot \mathbf{a}$. Finally define the set

$$\mathcal{M}_p(P_0) = \begin{cases} \emptyset & \text{if } v_1 X^e - v_c \text{ has no linear} \\ & \text{factors for some } c \in \{2, \ldots, d\}, \\ \left\{ \begin{pmatrix} E_0 \\ E_{(i_2,\ldots,i_d)} \end{pmatrix} : 1 \leq i_c \leq l_c \right\} & \text{otherwise.} \end{cases}.$$

Theorem 3.2.7. *Suppose $P_0 \in H$ and p is a rational prime satisfying* ***(p1)^{split},(p2)*** *and* ***(p3)^{ram}****. If $\overline{p^h A}$ has full rank and the reductions $\overline{E}$ for every element $E \in \mathcal{M}_p(P_0)$ have full column rank d over $\mathbb{F}_p$, or if $\mathcal{M}_p(P_0) = \emptyset$, then $B_p(P_0) \cap H = \{P_0\}$.*

Proof. Let $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. Since $P \neq P_0$ there exist integers $n_1, \ldots, n_r$, not all zero, such that

$$N[P - P_0] = n_1 D_1 + \ldots + n_r D_r$$

in $J(\mathbb{K})$. Let τ_c be a well-behaved uniformizer for C_c at P_0, for $c \in \{1, \ldots, d\}$. Now

$$(n_1/N) \int_0^{D_1} \omega_f^c + \ldots + (n_r/N) \int_0^{D_r} \omega_f^c = \int_0^{[P-P_0]} \omega_f^c = \alpha_c^{(f)} t_c + \beta_c^{(f)} t_c^2$$

for $q \in \{1, \ldots, r\}$. Writing this in terms of matrices we get

$$A \cdot \mathbf{n} = \mathbf{a} \cdot \mathbf{t} + \mathbf{b} \cdot \mathbf{t}',$$

where $\mathbf{t}$ and $\mathbf{t}'$ are the column vectors $(t_1, \ldots, t_d)$ and $\left(t_1^2, \ldots, t_d^2\right)$ respectively. As in the unramified case, we have a matrix U such that $\overline{U \cdot (p^h A)} \equiv \mathbf{0}$ modulo p, but since $\overline{p^h A}$ has full rank, we can use Hensel's lemma to lift U to a matrix $\hat{U}$ such that $\overline{U} \equiv \overline{\hat{U}}$ and $\hat{U} \cdot A = \mathbf{0}$. So we have that

$$\mathbf{0} = \hat{U} \cdot \mathbf{a} \cdot \mathbf{t} + \hat{U} \cdot \mathbf{b} \cdot \mathbf{t}'.$$

Dividing by p^s, reducing modulo p and denoting $\overline{(1/p^s)\mathbf{t}}$ by $\mathbf{v}$ we see that

$$\mathbf{0} \equiv \overline{\hat{U} \cdot \mathbf{a}} \cdot \mathbf{v} \equiv \overline{E_0} \cdot \mathbf{v} \mod p, \tag{3.2.3}$$

since $s \geq 1$.

Also we can write $\psi(P) - \psi(P_0)$ as a powerseries in t_c for every c. Since the ramification index of $\psi^{\mathfrak{p}_c}$ at P_0 is e by $(\mathrm{p3})^{\mathrm{ram}}$, these powerseries will all start from the

e-th term. Using these expansions we get the d equalities

$$\psi(P) - \psi(P_0) = \upsilon_c t_c^e + \rho_c t_c^{e+1}.$$

By Lemma 3.2.6 we know that there exist $i_c \in \{1, \ldots, l_c\}$ for each $c \in \{2, \ldots, d\}$ such that

$$t_1 - \hat{\gamma}_c^{(i_c)} t_c \equiv 0 \mod p^{2s},$$

where $s = \mathrm{ord}_p(t_1) = \ldots = \mathrm{ord}_p(t_d)$. Since $s \geq 1$ we get that

$$t_1 - \hat{\gamma}_c^{(i_c)} t_c \equiv 0 \mod p^{s+1}.$$

This can be re-written as

$$\mathbf{0} \equiv E_{(i_2,\ldots,i_d)}\mathbf{t} \mod p^{s+1}.$$

Dividing by p^s and reducing modulo p we obtain that

$$\mathbf{0} \equiv \overline{E_{(i_1,\ldots,i_d)}}\mathbf{v} \mod p. \tag{3.2.4}$$

Relations (3.2.3) and (3.2.4) put together imply that there exists $E \in \mathcal{M}_p(P_0)$ with

$$\mathbf{0} \equiv \overline{E}\mathbf{v} \mod p.$$

But this is a contradiction since $\mathrm{rank}_{\mathbb{F}_p}(\overline{E}) = d$ and $\mathbf{v} \not\equiv 0 \mod p$. □

p inert

Now if we assume that $\mathbb{K}$ is a quadratic extension of $\mathbb{Q}$ the following results show how we may also use an odd rational prime p which is inert in $\mathbb{K}$. This might prove useful in practice, since a split prime satisfying the properties $\mathbf{(p1)^{split}}$,$\mathbf{(p2)}$ and $\mathbf{(p3)^{ram}}$, might be too big for computational purposes. In the following results we denote by $\mathfrak{p}$

the unique prime above p, which has norm p^2, by $\mathbb{K}_\mathfrak{p}$ the completion of $\mathbb{K}$ with respect to $\mathfrak{p}$ and by $\mathcal{O}_\mathfrak{p}$ the ring of integers of $\mathbb{K}_\mathfrak{p}$. Let $\mathcal{C}$ be a minimal, regular and proper model for $C_\mathfrak{p} = C \times_\mathbb{K} \mathbb{K}_\mathfrak{p}$ over $\mathcal{O}_\mathfrak{p}$.

Lemma 3.2.8. *Suppose that* $[\mathbb{K} : \mathbb{Q}] = 2$, $P_0 \in H$ *and* p *is a rational prime that satisfies* ***(p1)^{inert},(p2)*** *and* ***(p3)^{ram}****. Let* τ *be a well-behaved uniformizer of* $C_\mathfrak{p}$ *at* P_0 *and denote by*

$$\upsilon T^e + \sum_{i=1}^{\infty} \rho_i T^{e+i} \in \mathbb{K}_\mathfrak{p}[[T]]$$

the formal expansion of $\psi^\mathfrak{p} - \psi(P_0)$ *in terms of* τ*. Write*

$$(v_1\theta_1 + v_2\theta_2)(T_1\theta_1 + T_2\theta_2)^e = W_1(T_1, T_2)\theta_1 + W_2(T_1, T_2)\theta_2,$$

where v_1, v_2, T_1 *and* T_2 *are defined by* $\upsilon = v_1\theta_1 + v_2\theta_2$ *and* $T = T_1\theta_1 + T_2\theta_2$, *and* $W_1, W_2 \in \mathbb{Z}_p[T_1, T_2]$ *are forms of degree* e*. Suppose further that* $\mathrm{ord}_p(\Delta) = 0$, *where* Δ *is the discriminant of* W_2*. Then if there exists* $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$, W_2 *has a linear factor* $g_1T_1 - g_2T_2$ *satisfying*

$$g_1t_1 - g_2t_2 \equiv 0 \mod p^{2s},$$

where t_1, t_2 *are defined by* $\tau(P) = t_1\theta_1 + t_2\theta_2$ *and* $1 \leq s = \min(\mathrm{ord}_p(t_1), \mathrm{ord}_p(t_2)) < \infty$.

Proof. By substituting P in the powerseries expansion of $\psi^\mathfrak{p} - \psi(P_0)$ we get

$$\begin{aligned} \psi^\mathfrak{p}(P) - \psi(P_0) &= (W_1(t_1, t_2)\theta_1 + W_2(t_1, t_2)\theta_2) + \\ &\quad (W_3(t_1, t_2)\theta_1 + W_4(t_1, t_2)\theta_2), \end{aligned}$$

where $W_3, W_4 \in \mathbb{Z}_p[[t_1, t_2]]$ are powerseries whose degree (as powerseries) is greater than e. Note that we used the fact that $\rho_i \in \mathcal{O}_\mathfrak{p}$ for every i (see Lemma 3.2.5). Since $\psi(P) \in \mathbb{Q}$, we have that

$$W_2(t_1, t_2) = -W_4(t_1, t_2).$$

Furthermore since $P \neq P_0$ either $t_1 \neq 0$ or $t_2 \neq 0$, so $s := \min(\mathrm{ord}_p(t_1), \mathrm{ord}_p(t_2))$ is finite. Combining this with the fact that $\mathrm{ord}_{\mathfrak{p}}(\tau(P)) \geq 1$ we can see that s is actually a positive integer. We have that

$$W_2(t_1, t_2) \equiv 0 \mod p^{s(e+1)}.$$

By Hensel's lemma (since $\mathrm{ord}_p(\Delta) = 0$) we have that there exist $g_1, g_2 \in \mathbb{Z}_p$ such that

$$(g_1 T_1 - g_2 T_2) \mid W_2(T_1, T_2)$$

and

$$g_1 t_1 - g_2 t_2 \equiv 0 \mod p^{2s}.$$

□

Let $\mathbb{K}, P_0, e, p, t_1, t_2, W_2$ be as in the statement of Lemma 3.2.8 above. Suppose that $(g_1^{(1)} T_1 - g_2^{(1)} T_2), \ldots, (g_1^{(l)} T_1 - g_2^{(l)} T_2)$ are all the linear factors of $W_2(T_1, T_2)$. Define the l matrices $E_{(i)} \in M_{1,2}(\mathbb{Z}_p)$ by

$$E_{(i)} = \begin{pmatrix} g_1^{(i)} & -g_2^{(i)} \end{pmatrix}$$

for $i \in \{1, \ldots, l\}$.

Let $\{\omega_f\}_{1 \leq f \leq g}$ be a basis of $H^0(\mathcal{C}, \Omega^1)$, $\{\theta_1, \theta_2\}$ be an integral basis of $\mathcal{O}_{\mathfrak{p}}$ over $\mathbb{Z}_p$, and $L = \langle D_1, \ldots, D_r \rangle$ be a subgroup of $J(\mathbb{K})$ of index $N \in \mathbb{Z}_{>0}$. Define $\{A^{(1)}, \ldots, A^{(g)}\} \subseteq M_{2,r}(\mathbb{Q}_p)$ to be the matrices whose entries are defined by

$$A_{1,q}^{(f)} \theta_1 + A_{2,q}^{(f)} \theta_2 = \int_0^{D_q} \omega_f,$$

and for $f \in \{1, \ldots, g\}$ define $\mathbf{a}^{(f)} \in M_{2,2}(\mathbb{Z}_p)$ to be the matrix representing in coordinates $\alpha^{(f)}$, the coefficient of the linear term in the (formal) powerseries expansion of $\int_0^{[P - P_0]} \omega_f$

in terms of the uniformizer τ of $C_{\mathfrak{p}}$ at P_0. Now let A be the $2g \times r$ matrix

$$A = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(g)} \end{pmatrix}$$

with entries in $\mathbb{Q}_p$ and $\mathbf{a}$ be the $2g \times 2$ matrix

$$\mathbf{a} = \begin{pmatrix} \mathbf{a}^{(1)} \\ \vdots \\ \mathbf{a}^{(g)} \end{pmatrix}$$

with entries in $\mathbb{Z}_p$. Let h be the smallest integer such that $p^h A$ has entries in $\mathbb{Z}_p$. Again let $U \in M_{2g-r,2g}(\mathbb{Z}_p)$ be a matrix such that

$$\overline{U \cdot (p^h A)} \equiv \mathbf{0} \qquad \mod p.$$

We denote by $E_0 \in M_{2g-r,2}(\mathbb{Z}_p)$ the matrix $U \cdot \mathbf{a}$. Finally define the set

$$\mathcal{M}_p(P_0) = \begin{cases} \emptyset & \text{, if } W_2(T_1, T_2) \text{ has no linear factors,} \\ \left\{ \begin{pmatrix} E_0 \\ E_{(i)} \end{pmatrix} : 1 \leq i \leq l \right\} & \text{, otherwise.} \end{cases}.$$

Theorem 3.2.9. *Suppose* $[\mathbb{K} : \mathbb{Q}] = 2$, $P_0 \in H$ *and* p *is a rational prime satisfying* ***(p1)^{inert},(p2),(p3)^{ram}*** *and that* W_2, Δ *are defined as in the statement of Lemma 3.2.8 with* $\mathrm{ord}_p(\Delta) = 0$. *Then if* $\overline{p^h A}$ *has full rank and* $\mathrm{rank}_{\mathbb{F}_p}(\overline{E}) = 2$ *for every* $E \in \mathcal{M}_p(P_0)$ *or if* $\mathcal{M}_p(P_0) = \emptyset$, *we have that* $B_p(P_0) \cap H = \{P_0\}$.

Proof. Let $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. Since $P \neq P_0$ there exist integers $n_1, \ldots, n_r$, not all zero, such that

$$N[P - P_0] = n_1 D_1 + \ldots + n_r D_r$$

in $J(\mathbb{K})$. Let τ be a well-behaved uniformizer for $C_{\mathfrak{p}}$ at P_0. Now

$$(n_1/N)\int_0^{D_1}\omega_f+\ldots+(n_r/N)\int_0^{D_r}\omega_f=\int_0^{[P-P_0]}\omega_f=\alpha^{(f)}\tau(P)+\beta^{(f)}\tau(P)^2$$

for $q\in\{1,\ldots,r\}$. Writing this in terms of matrices we get

$$A\cdot\mathbf{n}=\mathbf{a}\cdot\mathbf{t}+\mathbf{b}\cdot\mathbf{t}',$$

where $\mathbf{t}$ and $\mathbf{t}'$ are the column vectors $\mathbf{t}=(t_1,t_2)$ and $\mathbf{t}'=(t_1',t_2')$ with t_1',t_2' defined by $\tau(P)^2=t_1'\theta_1+t_2'\theta_2$. As in Lemma 1.3.32 and Theorems 3.2.3 and 3.2.7 we can lift U to a matrix $\hat{U}$ such that $\overline{U}\equiv\overline{\hat{U}}$ and $\hat{U}\cdot A=\mathbf{0}$. So

$$\mathbf{0}=\hat{U}\cdot\mathbf{a}\cdot\mathbf{t}+\hat{U}\cdot\mathbf{b}\cdot\mathbf{t}'.$$

Dividing by p^s, reducing modulo p and denoting $\overline{(1/p^s)\mathbf{t}}$ by $\mathbf{v}$, we see that

$$\mathbf{0}\equiv\overline{\hat{U}\cdot\mathbf{a}}\cdot\mathbf{v}\equiv\overline{E_0}\cdot\mathbf{v}\mod p,\tag{3.2.5}$$

since $s\geq 1$.

Also, we can write $\psi^{\mathfrak{p}}(P)-\psi^{\mathfrak{p}}(P_0)$ as a powerseries in $\tau(P)$. Since the ramification index of $\psi^{\mathfrak{p}}$ at P_0 is e by $(\mathrm{p3})^{\mathrm{ram}}$, this powerseries will start from the e-th term. By Lemma 3.2.8 we know that there exists $i\in\{1,\ldots,l\}$ such that

$$g_1^{(i)}t_1-g_2^{(i)}t_2\equiv 0\mod p^{2s},$$

where $s=\min\left(\mathrm{ord}_p(t_1),\mathrm{ord}_p(t_2)\right)$. Since $s\geq 1$ we get that

$$g_1^{(i)}t_1-g_2^{(i)}t_2\equiv 0\mod p^{s+1}.$$

This can be re-written as

$$\mathbf{0} \equiv E_{(i)} \cdot \mathbf{t} \mod p^{s+1}.$$

Dividing by p^s and reducing modulo p we obtain that

$$\mathbf{0} \equiv \overline{E_{(i)}} \cdot \mathbf{v} \mod p. \tag{3.2.6}$$

Relations (3.2.5) and (3.2.6) put together imply that there exists $E \in \mathcal{M}_p(P_0)$ with

$$\mathbf{0} \equiv \overline{E} \cdot \mathbf{v} \mod p.$$

But this is a contradiction since $\mathrm{rank}_{\mathbb{F}_p}(\overline{E}) = 2$ and $\mathbf{v} \not\equiv 0 \mod p$. □

3.2.3 Applying Chabauty

Example 3.2.10. Let $\mathbb{K}$ be the number field defined by $\mathbb{Q}[x]/(x^2 - x + 3)$, and denote by θ the corresponding image of x in the quotient. Consider the first three out of four genus 2 curves C_1, C_2 and C_3 defined in Example 3.1.4 by the equations

$$C_1 : \quad y^2 = x^5 + \theta x^4 - x^3 + x^2 + (\theta - 1)x - 1 \tag{3.2.7}$$

$$C_2 : \quad y^2 = -x^5 - \theta x^4 + x^3 - x^2 - (\theta - 1)x + 1 \tag{3.2.8}$$

$$C_3 : \quad y^2 = (-\theta + 5)x^5 + (4\theta + 3)x^4 + (\theta - 5)x^3 + (-\theta + 5)x^2 + (5\theta - 2)x + \theta - 5 \tag{3.2.9}$$

and the "x-coordinate" maps $\psi_{C,1}, \psi_{C,2}, \psi_{C,3}$ from the projective models of these curves (whose points will be denoted by $(X, Y, Z) \in \mathbb{P}^2(2, 5, 1)$) to the projective line

$$\psi_{C,i} : C_i \to \mathbb{P}^1, \quad \psi_{C,i}(X, Y, Z) = \left(X, Z^2\right).$$

Denote $C_i(\mathbb{K}) \cap \psi_{C,i}^{-1}\left(\mathbb{P}^1(\mathbb{Q})\right)$ by H_i for $1 \leq i \leq 3$. Let

$$\begin{aligned} H_1^{\text{search}} &:= \{(-1,-1,1),(-1,1,1),(1,1,0)\} \subseteq H_1 \\ H_2^{\text{search}} &:= \{(0,1,1),(0,-1,1),(-1,1,0)\} \subseteq H_2 \\ H_3^{\text{search}} &:= \{(1,\sqrt{5-\theta},0)\} \subseteq H_3. \end{aligned} \tag{3.2.10}$$

After searching for $\mathbb{K}$-rational points on C_1, C_2 and C_3 it appears that actually $H_1^{\text{search}} = H_1, H_2^{\text{search}} = H_2$ and $H_3^{\text{search}} = H_3$. The first step towards proving this is using Theorems 3.2.3, 3.2.7 and 3.2.9 together with the relevant information (computed using MAGMA [4]) presented in the following tables:

In TABLE 3.1 we observe that the rank of the Mordell-Weil group of the Jacobian variety of C_1 is equal to $3 > d(g-1) = 2$, making it impossible to use the classical method of Chabauty, improved by Siksek, which requires that $r \leq d(g-1)$. See for example [48]. Our approach is applicable in cases where the rank r of $J(\mathbb{K})$ satisfies

$$r \leq dg - 1.$$

In TABLE 3.2 we give the matrix A with entries in $\mathbb{Q}_p$ and a corresponding matrix U with entries in $\mathbb{Z}_p$, such that $\overline{U \cdot (p^h A)} \equiv \mathbf{0} \mod p$.

C	$\text{rank}_{\mathbb{F}_2}\left(\text{Sel}^{(2)}(J/\mathbb{K})\right)$	lin. ind. non-torsion divisors (In Mumford Representation)	$\text{rank}\,(J(\mathbb{K}))$
C_1	3	$(x^2-x+1,-x+1)$ $(x^2+(\theta-1)x-1,(\theta-1)x-1)$ $(x^2+(-\theta-1)x-\theta+2,(3\theta-1)x+\theta-4)$	3
C_2	1	$(x^2-x-\theta,(\theta-2)x-2)$	1
C_3	1	$(x^2+(2\theta-1)x+\theta-3,(-4\theta-3)x-5\theta+2)$	1

Table 3.1: The Mordell-Weil data for C_1, C_2 and C_3.

Using Theorems 3.2.3, 3.2.7 and the data in TABLES 3.3, 3.4 and 3.5 we deduce the following:

	p	A	U
C_1	89	$\begin{pmatrix} 70 & 82 & 51 \\ 70 & 61 & 86 \\ 55 & 3 & 58 \\ 29 & 38 & 28 \end{pmatrix} \times 89 + O(89^2)$	$\begin{pmatrix} 6 & 2 & -6 & -11 \end{pmatrix}$
C_2	23	$\begin{pmatrix} -6 \\ -11 \\ -11 \\ -11 \end{pmatrix} \times 23 + O(23^2)$	$\begin{pmatrix} 1 & 0 & 11 & 1 \\ -11 & 0 & 6 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$
C_3	71	$\begin{pmatrix} 58 \\ 60 \\ 47 \\ 48 \end{pmatrix} \times 71 + O(71^2)$	$\begin{pmatrix} 1 & 0 & -13 & 13 \\ 0 & 1 & -11 & 11 \\ 0 & 0 & 23 & -24 \end{pmatrix}$

Table 3.2: The period matrices for C_1, C_2 and C_3.

(a) $B_{89}(P_0) \cap H_1 = \{P_0\}$ for every $P_0 \in H_1^{\text{search}}$

(b) $B_{23}(P_0) \cap H_2 = \{P_0\}$ for every $P_0 \in H_2^{\text{search}}$

(c) $B_{71}(P_0) \cap H_3 = \{P_0\}$ for every $P_0 \in H_3^{\text{search}}$

⊠

3.3 Mordell-Weil sieve

The idea behind the Mordell-Weil sieve was presented in Section 1.3.4. Here we provide an improved version, that applies to the scenario we are considering: We are interested in excluding residue classes $\mathcal{B}_p(\mathcal{P})$, for $\mathcal{P} \in \mathcal{H} \subseteq \prod_{\mathfrak{p}|p} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$, that have empty intersection with the set H^{search}, by showing that they actually have empty intersection with the set H. We rename the prime p appearing in the previous section by p_0 and we use it as the first prime in a finite sequence of primes $\{p_0, \ldots, p_b\}$. Theorem 3.3.1 is all we actually need, but the efficiency of the computation tends to depend a lot on the ordering of these primes. Experimental evidence shows that it is usually efficient to order the primes in decreasing order of "smoothness" of the sizes of the sets of rational points of the Jacobian

P_0	τ	$\mathbf{a}$	$\{E_{j_2}\}$	$\mathcal{M}_p(P_0)$
$(1,1,-1)$ unramified	$x+1$	$\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} + O(89)$	N/A	$\begin{pmatrix} 9 \end{pmatrix} + O(89)$
$(1,-1,-1)$ unramified	$x+1$	$\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} + O(89)$	N/A	$\begin{pmatrix} -9 \end{pmatrix} + O(89)$
$(1,1,0)$ ramified	$\frac{(\theta-1)x^2}{2y}$	$\begin{pmatrix} 0 & 0 \\ 41 & 0 \\ 0 & 0 \\ 0 & 79 \end{pmatrix} + O(89)$	$\begin{pmatrix} 1 & 41 \end{pmatrix} + O(89)$, $\begin{pmatrix} 1 & -41 \end{pmatrix} + O(89)$	$\begin{pmatrix} 82 & 21 \\ 1 & 41 \end{pmatrix} + O(89)$, $\begin{pmatrix} 82 & 21 \\ 1 & -41 \end{pmatrix} + O(89)$

Table 3.3: Chabauty data for C_1

varieties over the residue fields. This usually results in large common divisors, which are needed to obtain contradictions in CRT-like arguments.

$$\begin{array}{ccccc} H & \subseteq & C(\mathbb{K}) & \xrightarrow{\quad\iota\quad} & J(\mathbb{K}) \\ \downarrow{\scriptstyle \mathrm{Red}_{p_i}} & & \downarrow{\scriptstyle \mathrm{Red}_{p_i}} & & \downarrow{\scriptstyle \mathrm{Red}_{p_i}} \\ \mathcal{H}_i & \subseteq & \prod_{\mathfrak{p}\mid p_i} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) & \xrightarrow{\quad\iota\quad} & \prod_{\mathfrak{p}\mid p_i} \overline{J}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) \end{array} \tag{3.3.1}$$

Theorem 3.3.1. *Let $L = \langle D_1, \ldots, D_r \rangle < J(\mathbb{K})$ be a subgroup of the Mordell-Weil group of finite index equal to N and $p_0, p_1, \ldots, p_b$ be rational primes satisfying*

(i) p_i does not ramify in $\mathcal{O}_{\mathbb{K}}$ for $0 \leq i \leq b$.

(ii) $C_{\mathfrak{p}}$ has good reduction for every prime $\mathfrak{p} \mid p_i$, for $0 \leq i \leq b$.

(iii) $\#\prod_{\mathfrak{p}\mid p_i} \overline{J}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ is coprime with N for $0 \leq i \leq b$.

Let

$$\mathcal{H}_i = \left\{ \mathcal{P} \in \prod_{\mathfrak{p}\mid p_i} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) : \overline{\psi^{\mathfrak{p}}}(\mathcal{P}_{\mathfrak{p}}) = \psi_{\mathfrak{q}}(\mathcal{P}_{\mathfrak{q}}) \in \mathbb{P}^1(\mathbb{F}_{p_i}) \quad \forall \mathfrak{p}, \mathfrak{q} \mid p_i \right\}.$$

P_0	τ	$\mathbf{a}$	$\{E_{j_2}\}$	$\mathcal{M}_p(P_0)$
$(0,-1,1)$ unramified	x	$\begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + O(23)$	N/A	$\begin{pmatrix} 11 \\ 5 \\ 1 \end{pmatrix} + O(23)$
$(0,1,1)$ unramified	x	$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + O(23)$	N/A	$\begin{pmatrix} -11 \\ -5 \\ -1 \end{pmatrix} + O(23)$
$(-1,1,0)$ ramified	$-\frac{\theta+2}{6}\frac{x^2}{y}$	$\begin{pmatrix} 0 & 0 \\ 17 & 0 \\ 0 & 0 \\ 0 & 5 \end{pmatrix} + O(23)$	$\begin{pmatrix} 1 & 3 \end{pmatrix} + O(23)$, $\begin{pmatrix} 1 & -3 \end{pmatrix} + O(23)$	$\begin{pmatrix} 0 & 5 \\ 0 & 0 \\ -6 & 0 \\ 1 & 3 \end{pmatrix} + O(23)$, $\begin{pmatrix} 0 & 5 \\ 0 & 0 \\ -6 & 0 \\ 1 & -3 \end{pmatrix} + O(23)$

Table 3.4: Chabauty data for C_2

P_0	τ	$\mathbf{a}$	$\{E_{j_2}\}$	$\mathcal{M}_p(P_0)$
$(1,\sqrt{5-\theta},0)$ ramified	$\frac{2(5-\theta)x^2}{y}$	$\begin{pmatrix} 0 & 0 \\ 56 & 0 \\ 0 & 0 \\ 0 & 64 \end{pmatrix} + O(71)$	$\emptyset$	$\emptyset$

Table 3.5: Chabauty data for C_3

Let $L_0 := L \cap \text{Kernel}\,(\text{Red}_{p_0})$ *and define inductively* $L_i := L_{i-1} \cap \text{Kernel}\,(\text{Red}_{p_i})$ *for* $1 \leq i \leq b$. *Then for every* $\mathcal{P} \in \mathcal{H}_0$ *define* $W_{0,\mathcal{P}} = \{l \in L/L_0 : \text{Red}_{p_0}(w) = \iota(\mathcal{P})\}$ *and then inductively* $W_{i,\mathcal{P}} := \{w + l : w \in W_{i-1,\mathcal{P}}, l \in L_{i-1}/L_i, \text{Red}_{p_i}(w+l) \in \iota(\mathcal{H}_i)\}$ *for* $1 \leq i \leq b$. *Then if* $W_{b,\mathcal{P}} = \emptyset$ *we have that* $\mathcal{B}_{p_0}(\mathcal{P}) \cap H = \emptyset$.

Proof. Suppose there exists some point P in $\mathcal{B}_{p_0}(\mathcal{P}) \cap H$. Then $N \cdot \iota(P) = n_1 D_1 + \ldots + n_r D_r$ for some $n_1, \ldots, n_r \in \mathbb{Z}$. Since condition (iii) holds for p_0 we have that $\text{Red}_{p_0}(\iota(P)) \in \text{Red}_{p_0}(L)$ and also $\text{Red}_{p_0}(\iota(P)) = \iota(\mathcal{P})$ by commutativity of diagram (3.3.1), in other words we can find $w_{0,P} \in L/L_0$ such that $\text{Red}_{p_0}(w_{0,P}) = \text{Red}_{p_0}(\iota(P))$. In particular $w_{0,P} \in W_{0,\mathcal{P}}$. Now suppose that for $i = 0, \ldots, i-1$ we have $w_{i-1,P} \in W_{i-1,\mathcal{P}}$

such that $\mathrm{Red}_{p_{i-1}}(w_{i-1,P}) = \mathrm{Red}_{p_{i-1}}(\iota(P))$. We now have

$$\iota(P) - w_{i-1,P} \in \bigcap_{j=0}^{i-1} \mathrm{Kernel}\left(\mathrm{Red}_{p_j}\right).$$

If we multiply by the index N we have

$$N\left(\iota(P) - w_{i-1,P}\right) \in L \cap \left(\bigcap_{j=0}^{i-1} \mathrm{Kernel}\left(\mathrm{Red}_{p_j}\right)\right) = L_{i-1}$$

and if we reduce both sides modulo p_i we get

$$N\,\mathrm{Red}_{p_i}\left(\iota(P) - w_{i-1,P}\right) \in \mathrm{Red}_{p_i}\left(L_{i-1}\right).$$

But since N is coprime with $\#\,\mathrm{Red}_{p_i}(L_{i-1})$ by (iii) this implies that

$$\mathrm{Red}_{p_i}\left(\iota(P) - w_{i-1,P}\right) \in \mathrm{Red}_{p_i}\left(L_{i-1}\right).$$

So there exists $l \in L_{i-1}/L_i$ such that $\mathrm{Red}_{p_i}(l) = \mathrm{Red}_{p_i}(\iota(P) - w_{i-1,P})$. But we can now define an element of $W_{i,\mathcal{P}}$ by

$$w_{i,P} := w_{i-1,P} + l \in W_{i,\mathcal{P}}.$$

In particular $W_{b,\mathcal{P}}$ is non-empty. □

Example 3.3.2. Let C_1, C_2 and C_3 be the curves defined in Example 3.1.4 by the equations (3.1.3),(3.1.4) and (3.1.5). Then

(a) $\mathcal{B}_{89}(\mathcal{P}) \cap H_1 = \emptyset$ for every $\mathcal{P} \in \prod_{\mathfrak{p}|89} \overline{C}_{1,\mathfrak{p}}(\mathbb{F}_\mathfrak{p}) \setminus \mathrm{Red}_{89}\left(H_1^{\mathrm{search}}\right)$. This was shown after taking $\{p_0, p_1, p_2, p_3 = p_b\} = \{89, 673, 859, 131\}$ and using Theorem 3.3.1 after checking that conditions $(i), (ii)$ and (iii) were satisfied for each of these primes.

(b) $\mathcal{B}_{23}(\mathcal{P}) \cap H_2 = \emptyset$ for every $\mathcal{P} \in \prod_{\mathfrak{p}|23} \overline{C}_{2,\mathfrak{p}}(\mathbb{F}_\mathfrak{p}) \setminus \mathrm{Red}_{23}\left(H_2^{\mathrm{search}}\right)$. The primes used here

were $\{23, 43\}$.

(c) $\mathcal{B}_{71}(\mathcal{P}) \cap H_3 = \emptyset$ for every $\mathcal{P} \in \prod_{\mathfrak{p}|71} \overline{C}_{3,\mathfrak{p}}(\mathbb{F}_\mathfrak{p}) \setminus \mathrm{Red}_{71}\left(H_3^{\mathrm{search}}\right)$. The primes used were $\{71, 131\}$.

⊠

Lemma 3.3.3. *Let C_1, C_2 and C_3 be the curves defined by equations* (3.1.3), (3.1.4) *and* (3.1.5) *respectively and let $\psi_{C,i}$ for $1 \leq i \leq 3$ be the corresponding "x-coordinate" maps from the curves to the projective line. We have that $H_i = \psi_{C,i}^{-1}\left(\mathbb{P}^1(\mathbb{Q})\right) \cap C_i(\mathbb{K}) = H_i^{\mathrm{search}}$ for $1 \leq i \leq 3$, where the H_i^{search} are as in* (3.2.10).

Proof. Just note that the corresponding parts of Examples 3.2.10 and 3.3.2 together give the required result. □

3.4 Applications to Diophantine problems

In this section we consider an example of a curve Υ defined over $\mathbb{Q}$ whose set of rational points is computed using the methods presented in the previous sections. This illustrates how all of the existing techniques ([6],[11],[13],[48]) may fail due to theoretical or computational restrictions[5], while the methods in this chapter remain applicable. Their usefulness should be more apparent when applied on curves that are not hyperelliptic, for example more general superelliptic curves. These might have Jacobians of Mordell-Weil rank large enough to pose a theoretical obstruction to the use of classical Chabauty or its refinement in [48] and also fail to be related to collections of curves of genus 1, where "Elliptic Curve Chabauty" might be applicable.

3.4.1 The equation $y^2 = (x^3 + x^2 - 1)\Phi_{11}(x)$

We can now prove the following

[5]We used the *RankBound* command in MAGMA to get that 1 is an upper bound for the Mordell-Weil rank over $\mathbb{Q}$ of the Jacobian variety of Υ. Thus, the explicit version of Chabauty-Coleman would be applicable if we could find a generator. But even after extensive search, a generator could not be found.

Theorem 3.4.1. *The only $\mathbb{Q}$-rational point on the curve Υ defined by the equation*

$$\Upsilon : \quad y^2 = (x^3 + x^2 - 1)\Phi_{11}(x)$$

is the point at infinity.

Proof. In Example 3.1.4 we saw that

$$\Upsilon(\mathbb{Q}) = \bigcup_{i=1}^{4} \phi_{\Upsilon,i}(D_i(\mathbb{Q})),$$

and also that

$$D_i(\mathbb{Q}) \subseteq \phi_{C,i}^{-1}(H_i),$$

where

$$H_i = \psi_{C,i}^{-1}(\mathbb{P}^1(\mathbb{Q})) \cap C_i(\mathbb{K}).$$

From Lemma 3.3.3 we know that $H_i = H_i^{\text{search}}$ for $1 \leq i \leq 3$. Also a 2-Selmer group computation shows that $J_4(\mathbb{K}) = \{0\}$, where J_4 is the Jacobian variety of C_4 and thus $H_4 = C_4(\mathbb{K}) = \{(1, \sqrt{\theta - 5}, 0)\}$. We should note that the points on the D_i's are defined as $(X, Y_1, Y_2, Y_3, Z) \in \mathbb{P}^4(2, 3, 5, 5, 1)$, with $\mathcal{G}_{\mathbb{Q}}$ acting on Y_2 and Y_3 the same way it acts on the roots of the defining polynomial of $\mathbb{K}$, and the points on the C_i's are defined as $(X, Y, Z) \in \mathbb{P}^2(2, 5, 1)$. To save space we fix a square root for each of -1, 23, $\theta - 5$ and $\theta + 4$ and denote them by ξ_1, ξ_2, ξ_3 and ξ_4 respectively. Putting these together we get the following:

$$D_1(\mathbb{Q}) \subseteq \phi_{C,1}^{-1}\left(\left\{\begin{array}{c}(-1,-1,1),\\(-1,1,1),\\(1,1,0)\end{array}\right\}\right)$$

$$= \left\{\begin{array}{l}(-1,\xi_1,-1,-1,1),(-1,-\xi_1,-1,-1,1),(-1,\xi_1,-1,1,1),(-1,-\xi_1,-1,1,1),\\(-1,\xi_1,1,1,1),(-1,-\xi_1,1,1,1),(-1,\xi_1,1,-1,1),(-1,-\xi_1,1,-1,1),\\(1,1,1,1,0),(1,-1,1,1,0),(1,1,1,-1,0),(1,-1,1,-1,0)\end{array}\right\}$$

$$\Rightarrow D_1(\mathbb{Q}) = \{(1,1,1,1,0),(1,-1,1,1,0)\}$$

$$D_2(\mathbb{Q}) \subseteq \phi_{C,2}^{-1}\left(\left\{\begin{array}{c}(0,-1,1),\\(0,1,1),\\(-1,1,0)\end{array}\right\}\right)$$

$$= \left\{\begin{array}{l}(0,\xi_1,-1,-1,1),(0,-\xi_1,-1,-1,1),(0,\xi_1,-1,1,1),(0,-\xi_1,-1,1,1),\\(0,\xi_1,1,1,1),(0,-\xi_1,1,1,1),(0,\xi_1,1,-1,1),(0,-\xi_1,1,-1,1),\\(-1,\xi_1,1,1,0),(-1,-\xi_1,1,1,0),(-1,\xi_1,1,-1,0),(-1,-\xi_1,1,-1,0)\end{array}\right\}$$

$$\Rightarrow D_2(\mathbb{Q}) = \emptyset$$

$$D_3(\mathbb{Q}) \subseteq \phi_{C,3}^{-1}\left(\left\{\ (1,\xi_1\xi_3,0)\ \right\}\right)$$

$$= \left\{\ (1,\xi_2,\xi_1\xi_3,\xi_4,0),(1,-\xi_2,\xi_1\xi_3,\xi_4,0),(1,\xi_2,\xi_1\xi_3,-\xi_4,0),(1,-\xi_2,\xi_1\xi_3,-\xi_4,0)\ \right\}$$

$$\Rightarrow D_3(\mathbb{Q}) = \emptyset$$

$$D_4(\mathbb{Q}) \subseteq \phi_{C,4}^{-1}\left(\left\{\ (1,\xi_3,0)\ \right\}\right)$$

$$= \left\{\ (1,\xi_2,\xi_3,\xi_1\xi_4,0),(1,-\xi_2,\xi_3,\xi_1\xi_4,0),(1,\xi_2,\xi_3,-\xi_1\xi_4,0),(1,-\xi_2,\xi_3,-\xi_1\xi_4,0)\ \right\}$$

$$\Rightarrow D_4(\mathbb{Q}) = \emptyset$$

So we have that $\Upsilon(\mathbb{Q}) = \phi_{\Upsilon,1}(D_1(\mathbb{Q})) = \{(1,1,0) = \infty\}$. $\square$

Remark 3.4.2. The MAGMA functions used to tackle this problem, along with comments explaining how they work, can be found at

`http://www.warwick.ac.uk/~marfaq/chabauty.m`.

This can be easily adapted to work with other examples, but currently the polynomial defining Υ must have a quintic or a sextic factor (depending on whether the initial degree is odd or even respectively) over a quadratic number field. ⊠

Chapter 4

Future Directions

We will conclude this thesis by presenting some ways the techniques developed in Chapters 2 and 3 can be refined.

4.1 Finding uniform bounds using extended Chabauty-Coleman

Another interesting direction to consider, would be to find uniform bounds on the size of the set $H = \psi^{-1}(\mathbb{P}^1(\mathbb{Q})) \cap C(\mathbb{K})$ used in Chapter 3. This may be applicable to further improve existing bounds on the size of the set of rational points of different classes of curves (see for example the use of Chabauty's method to bound the number of points on hyperelliptic curves in [13] and the number of solutions of Thue equations in [35]).

The new bounds should depend only on the number of zeros a holomorphic differential $\overline{\omega}$ has on $\overline{C}_{\mathfrak{p}}$ and the size of the set

$$\mathcal{H} = \{\mathcal{P} \in \prod_{\mathfrak{p}|p} \overline{C}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) : \overline{\psi^{\mathfrak{p}}}(\mathcal{P}_{\mathfrak{p}}) = \overline{\psi^{\mathfrak{q}}}(\mathcal{P}_{\mathfrak{q}}) \in \mathbb{P}^1(\mathbb{F}_p) \quad \forall \mathfrak{p}, \mathfrak{q} \mid p\},$$

in the same way the current bounds depend on the number of zeros of differentials and $\#C(\mathbb{F}_{\mathfrak{p}})$ (as in Theorem 1.3.28).

4.2 Explicit Chabauty-Coleman on superelliptic curves

Along with the more theoretical directions, one could consider providing an explicit description of how to apply Chabauty-Coleman techniques on particular examples of superelliptic curves. This will open the door to a complete solution of an abundance of interesting Diophantine equations (e.g. unsolved cases of the Generalized Fermat equation $X^p + Y^q = Z^r$). Most of the theoretical groundwork needed to do this has already been laid out. Some of the issues that still need to be addressed are the following:

1. **Searching for points on J:** In order to find generators for a finite index subgroup of $J(\mathbb{K})$ one has to perform a search for $\mathbb{K}$-rational points on J. Currently this is only implemented for curves C with $g = 2$ and $\mathbb{K} = \mathbb{Q}$, using the Elkies-Stahlke-Stoll algorithm ([18],[53]) to search for points on the Kummer surface K. There is a straight-forward way to use the algorithm to search for higher degree divisors on higher genus hyperelliptic and superelliptic curves over any number field. It should be possible to refine this method further and improve its efficiency.

2. **Use of Kedlaya's algorithm for Chabauty-type computations:** When performing Chabauty's method it is crucial to efficiently compute $\mathfrak{p}$-adic integrals on $C_{\mathfrak{p}}$ and $J_{\mathfrak{p}}$. Although there are ways to do this indirectly (see for example [56]), the most efficient way to do this would be to introduce the use of Kedlaya's algorithm for computing Frobenius actions on de Rham cohomology ([31]), as was done in [1] for hyperelliptic curves, where it is also noticed that this could be generalized to superelliptic curves extending on the work done in [25].

3. **Arithmetic of points on J:** Performing the Mordell-Weil sieve requires knowledge of the finite group $\overline{J}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ as well as being able to solve the discrete logarithm problem for elements of this group. This issue, along with an explicit method to perform addition of points on the Jacobian as well as reduction of divisors to a canonical representative in the same class have been addressed in [24]. Another,

possibly more efficient and general, implementation of arithmetic on the Jacobian can be extracted from [32] and [33].

Combining (1) – (3) and the implementation of descent on the Jacobian[1], provides an algorithm for determining the set $C(\mathbb{K})$ for many examples of superelliptic curves C. We have worked out the details of how solving this problem for a particular collection of curves of this type will allow us to deal with the Generalized Fermat equation $X^7+Y^7 = Z^5$. But judging by how important the study of hyperelliptic curves proved to be in Diophantine Geometry, we can only be certain that the extension of these techniques to a more general class of curves will carry equal significance.

[1] The implementation in MAGMA of descent on the Jacobian varieties of cyclic covers of the projective line is now in its final stages, due to the work of Brendan Creutz.

Bibliography

[1] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31. MR 2721410

[2] Michael A. Bennett, *A superelliptic equation involving alternating sums of powers*, Publ. Math. Debrecen **79** (2011), no. 6.

[3] Michael A. Bennett, Kálmán Győry, and Ákos Pintér, *On the Diophantine equation* $1^k + 2^k + \cdots + x^k = y^n$, Compos. Math. **140** (2004), no. 6, 1417–1431. MR 2098395 (2005g:11042)

[4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[5] Nils Bruin, *Chabauty Methods and Covering Techniques applied to Generalised Fermat Equations*, Ph.D. thesis, Universiteit Leiden, 1999.

[6] ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. MR 2011330 (2004j:11051)

[7] Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347. MR 2156713 (2006k:11118)

[8] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, (2012), arXiv:1205.4456v1.

[9] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR 2433884 (2009d:11100)

[10] ———, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. MR 2521292 (2010e:11059)

[11] Claude Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024. MR 0011005 (6,102e)

[12] Wei-Liang Chow, *The Jacobian variety of an algebraic curve*, Amer. J. Math. **76** (1954), 453–476. MR 0061421 (15,823a)

[13] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR 808103 (87f:11043)

[14] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. MR 782557 (86j:14014)

[15] Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, (2012), arXiv:1204.5803.

[16] S. Duquesne, *Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem*, Manuscripta Math. **108** (2002), no. 2, 191–204. MR 1918586 (2003e:11067)

[17] Manfred Einsiedler, Graham Everest, and Thomas Ward, *Periodic points for good reduction maps on curves*, Geom. Dedicata **106** (2004), 29–41. MR 2079832 (2005e:11085)

[18] Noam D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 33–63. MR 1850598 (2002g:11035)

[19] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935 (85g:11026a)

[20] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR 2103661 (2005j:11047)

[21] E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533. MR 1734798 (2001g:11098)

[22] ———, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205. MR 1831612 (2002b:11088)

[23] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR 1042981 (90k:14023)

[24] S. D. Galbraith, S. M. Paulus, and N. P. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002), no. 237, 393–405 (electronic). MR 1863009 (2002h:14102)

[25] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR 1934859 (2003h:11159)

[26] K. Győry, R. Tijdeman, and M. Voorhoeve, *On the equation* $1^k + 2^k + \cdots + x^k = y^z$, Acta Arith. **37** (1980), 233–240. MR 598878 (82h:10021)

[27] Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. MR 1915212 (2003h:11068)

[28] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)

[29] Helmut Hasse, *Über die darstellbarkeit von Zahlen durch quadratische Formen im Körber der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148.

[30] K. Hensel, *Theorie der algebraischen zahlen*, Cornell University Library historical math monographs, no. v. 1, B. G. Teubner, 1908.

[31] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338. MR 1877805 (2002m:14019)

[32] Kamal Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), no. 245, 333–357 (electronic). MR 2034126 (2005a:14081)

[33] ———, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. **76** (2007), no. 260, 2213–2239 (electronic). MR 2336292 (2009a:14072)

[34] Carl-Erik Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala, **1940** (1940), 97. MR 0022563 (9,225c)

[35] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR 1892843 (2003d:11088)

[36] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, (2007), available at `http://www-math.mit.edu/~poonen/papers/chabauty.pdf`.

[37] Louis Joel Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc Cam. Phil. Soc. **21** (1922), 179–192.

[38] Michael Mourao, *Extending Elliptic Curve Chabauty to higher genus curves*, (2011), arXiv:1111.5506.

[39] ———, *Descent on superelliptic curves*, (2012), arXiv:1010.2360v5.

[40] Ákos Pintér, *On the power values of power sums*, J. Number Theory **125** (2007), no. 2, 412–423. MR 2332596 (2008g:11052)

[41] Bjorn Poonen, *Rational points on varieties*, available at `http://www-math.mit.edu/~poonen/papers/Qpoints.pdf`, 2003, Lecture Notes, UC Berkeley.

[42] ———, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR 2293593 (2008d:11062)

[43] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR 1465369 (98k:11087)

[44] Hans Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18. MR 0009381 (5,141c)

[45] Juan J. Schäffer, *The equation* $1^p + 2^p + 3^p + \cdots + n^p = m^q$, Acta Math. **95** (1956), 155–189. MR 0078395 (17,1187a)

[46] Victor Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, Ph.D. thesis, University of Michigan, 1999.

[47] Ernst S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 (1 plate). MR 0041871 (13,13i)

[48] Samir Siksek, *Explicit chabauty over Number Fields*, (2011), arXiv:1010.2603v2.

[49] Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized fermat equation* $x^3 + y^4 + z^5 = 0$, Bulletin of the London Mathematical Society **44** (2012), no. 1, 151–166.

[50] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005)

[51] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR 1829626 (2002b:11089)

[52] Eduardo Tengan, *An Invitation to Local Fields*, (2008), available at `http://www.icmc.usp.br/~etengan/algebra/arquivos/lcft.pdf`.

[53] Mark Watkins, *Searching for points with the Elkies ANTS- IV algorithm*, `magma.maths.usyd.edu.au/~watkins/papers/padic.ps`.

[54] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315. MR 1555278

[55] ———, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948. MR 0027151 (10,262c)

[56] Joseph L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, 1998.